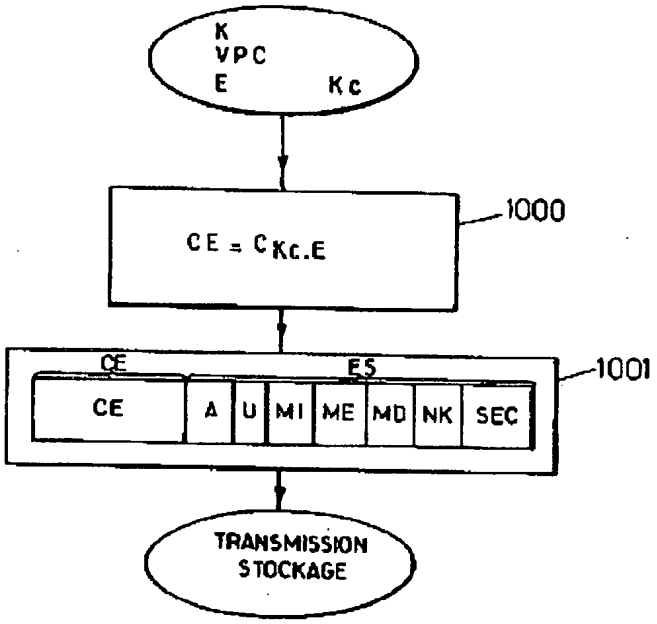
Protection of data that is to be transmitted over a network, e.g. the Internet has a stage where data is encoded using a physical key associated with the computer and a stage where an electronic signature is attached to it

Patent number:	FR2793903
Publication date:	2000-11-24
Inventor:	DELAHAYE JEAN PIERRE
Applicant:	TELEDIFFUSION FSE (FR)
Classification:	
- international:	G06F12/14
- european:	G06F1/00N7R, G06F21/00N7D, H04L9/32S
Application number:	FR19990006483 19990521
Priority number(s):	FR19990006483 19990521

Abstract of **FR2793903**

Procedure in which data to be encoded is encoded (1000) so that a set of encoded data (CE) is generated. An electronically signed envelope (ES) comprises an electronic signature associated (1001) with encoded data for transmission or stocking together. An Independent claim is made for a data protection system. Procedure is for a computer with a physical key that contains specific cryptographic parameters. All data processed by the computer is encoded using the cipher key and an electronically signed enveloped is associated with the data comprising non-encoded data such as a random number of p bits, an identification sign for verifying the existence of encoded data, a number representative of the physical key and a linked electronic signature (SEC).



(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 793 903**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **99 06483**

(51) Int Cl[7] : G 06 F 12/14

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 21.05.99.

(30) **Priorité** :

(43) **Date de mise à la disposition du public de la demande** : 24.11.00 Bulletin 00/47.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *TELEDIFFUSION DE FRANCE Société anonyme* — FR.

(72) **Inventeur(s)** : DELAHAYE JEAN PIERRE.

(73) **Titulaire(s)** :

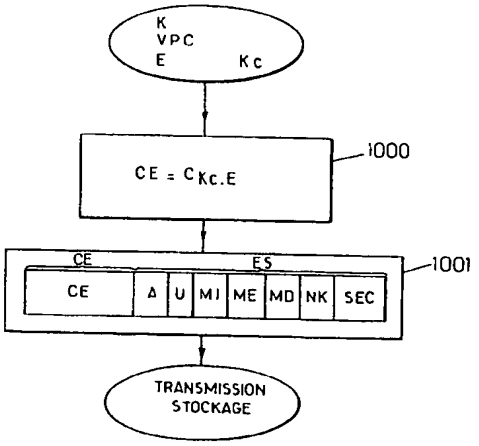
(74) **Mandataire(s)** : CABINET PLASSERAUD.

(54) PROCEDE ET SYSTEME DE SECURISATION DE DONNEES NUMERIQUES.

(57) L'invention concerne un procédé et un système de sécurisation de données.

Les données à chiffrer sont chiffrées (1000) pour engendrer un ensemble de données chiffrées (CE). Une enveloppe électronique signée (ES) comportant au moins une signature électronique conjointe (SEC) est associée (1001) aux données chiffrées pour transmission ou stockage de l'ensemble.

Application aux transactions en réseau, notamment de commerce électronique.



FR 2 793 903 - A1

PROCÉDÉ ET SYSTÈME DE SÉCURISATION DE DONNÉES NUMÉRIQUES

L'invention concerne un procédé et un système de sécurisation de données numériques traitées par un ordinateur, contre la copie, la modification ou l'utilisation illicites de ces données par des tiers non habilités.

La multiplication de l'échange de données de toute nature par l'intermédiaire de réseaux informatiques, tels que notamment le réseau *INTERNET*, pose le problème crucial de l'intégrité, de la fiabilité, de l'authenticité et de l'inviolabilité de ces données, afin d'assurer la sécurité et la fiabilité des transactions réalisées au cours de ces échanges.

Le problème de la fiabilité, de l'authenticité et de l'inviolabilité des données transmises se pose actuellement relativement à toutes les applications de commerce électronique, d'échange de documents confidentiels et/ou officiels pour lesquels toute interception, copie ou création frauduleuse est rédhibitoire pour un utilisateur autorisé.

A l'heure actuelle, la transmission de ce type de données de manière sécurisée, que cette transmission soit effectuée par l'intermédiaire de supports physiques par enregistrement de ces données sur ces supports physiques tels que disques souples, bandes magnétiques ou autres, ou d'une transmission de messages en réseaux, consiste essentiellement à effectuer une opération de chiffrement de ces données, au moyen de systèmes cryptographiques adaptés.

De tels systèmes donnent satisfaction, mais le niveau de protection des données sécurisées transmises dé-

pend uniquement de la difficulté à percer la convention de chiffrement utilisée et donc du degré de sécurité de cette dernière.

Plus récemment, des systèmes plus élaborés visant à protéger, non seulement les données transmises, mais également l'accès à la sécurisation de ces données, afin de réserver le processus de sécurisation de ces données aux seules personnes habilitées, ont été décrits notamment par la demande de brevet français n° 97 04340 publiée le 16 octobre 1998 sous le numéro 2 762 111 au nom de la demanderesse.

Le système décrit dans la demande de brevet précitée permet, à partir d'un ordinateur muni d'une clé physique de protection, encore appelée *"dongle"*, d'assurer une compression puis un embrouillage des données à sécuriser préalablement au stockage ou à la transmission des données ainsi sécurisées. Lors de l'utilisation de ces dernières, une opération de désembrouillage puis de décompression est effectuée à partir d'un ordinateur muni d'une clé physique de protection correspondante. Ces opérations peuvent en outre être rendues conditionnelles à l'introduction d'un mot de passe d'accès utilisateur implanté dans une carte à microprocesseur par exemple.

Un tel système donne satisfaction car il permet, d'une part, de sécuriser les données transmises par les opérations de compression/embrouillage, et, d'autre part, de sécuriser l'accès au processus de sécurisation par compression/embrouillage.

Toutefois, le niveau de sécurisation des données transmises par les opérateurs de compression/embrouillage ne peut être comparé au niveau de sécurisation de données

par chiffrement grâce à des processus de chiffrement à clé secrète ou privée et publique.

En outre, un tel système ne permet pas la mise en œuvre d'un processus systématique de vérification de l'intégrité des données sécurisées transmises, ni a fortiori la mise en œuvre d'un processus systématique d'authentification de l'origine de ces données, ni d'un processus de non-répudiation de la transaction relative à ces données sécurisées, en raison de l'absence, dans cette transaction, de données susceptibles de permettre l'authentification de l'origine de cette transmission.

La présente invention a pour objet de remédier aux inconvénients ou limitations des systèmes de sécurisation de données numériques de l'art antérieur précités.

En conséquence, la présente invention propose un procédé et un système de sécurisation de données numériques traitées par un ordinateur muni d'une clé physique de protection permettant de délivrer à cet ordinateur un code de clé physique et des valeurs spécifiques de paramétrage cryptographique.

Ils sont remarquables, pour tout ensemble de données numériques traitées, en ce qu'ils consistent à, respectivement permettent de chiffrer cet ensemble de données à partir d'au moins une clé de chiffrement, pour engendrer un ensemble de données chiffrées, et à associer à cet ensemble de données chiffrées une enveloppe électronique signée.

L'enveloppe électronique signée comporte au moins des paramètres non chiffrés tels qu'un aléa de p bits, un motif d'identification d'enveloppe électronique signée, codé sur s bits, calculé à partir d'au moins une des va-

leurs spécifiques de paramétrage cryptographique et permettant de vérifier l'existence d'un ensemble de données chiffrées associé à cette enveloppe électronique signée, et un numéro représentatif de la clé physique de protection équipant l'ordinateur. L'enveloppe signée comporte en outre une signature électronique conjointe, obtenue à partir d'une signature de l'ensemble de données chiffrées et d'une signature des paramètres non chiffrés de l'enveloppe électronique. Ceci permet, lors de l'utilisation des données chiffrées de cet ensemble de données chiffrées, de procéder à une vérification de l'authenticité des paramètres non chiffrés de l'enveloppe électronique signée, de l'intégrité de l'ensemble des données chiffrées et de l'enveloppe électronique signée, puis de déchiffrer les données chiffrées de cet ensemble de données chiffrées pour utilisation. Ces opérations sont réalisées dans la mesure où l'utilisateur détient les droits d'accès et d'usage des prestations cryptographiques proposées.

Le procédé et le système de sécurisation de données, objets de la présente invention, trouvent application à la sécurisation de données de toute nature dans des applications à des transactions de tout type.

Ils seront mieux compris à la lecture de la description et à l'observation des dessins dans lesquels :

- la figure 1a représente un schéma synoptique de mise en œuvre du procédé de sécurisation de données, objet de la présente invention ;

- la figure 1b représente, à titre d'exemple non limitatif, la structure de données constituant l'enveloppe électronique signée associée à l'ensemble des données chiffrées transmises conformément à l'objet de la présente

invention en vue de la transmission ou du stockage de ces dernières ;

- la figure 2a représente, à titre illustratif, un organigramme de calcul d'un champ spécifique de l'enveloppe électronique signée représentée en figure 1b, champ constitué par une signature électronique conjointe entre l'ensemble de données chiffrées et l'ensemble des paramètres non chiffrés constitutifs de l'enveloppe électronique signée ;

- la figure 2b représente, à titre d'exemple non limitatif, un mode de mise en œuvre préférentiel du processus de calcul de la signature électronique conjointe selon la figure 2a ;

- la figure 3a représente, à titre d'exemple illustratif, un organigramme général du processus de chiffrement de l'ensemble des données à chiffrer, à partir d'une suite chiffrante ;

- la figure 3b représente, à titre d'exemple illustratif, un organigramme spécifique relatif à la mise en œuvre du calcul de la suite chiffrante, utilisée pour le processus de chiffrement illustrée en figure 3a, dans un mode de réalisation préférentiel non limitatif ;

- la figure 3c représente, à titre illustratif, un organigramme spécifique relatif à la mise en œuvre de l'opération de chiffrement illustrée en figure 3a, dans un mode de réalisation préférentiel non limitatif correspondant à la mise en œuvre de la suite chiffrante selon la figure 3b ;

- la figure 3d représente, à titre illustratif, un organigramme spécifique relatif à la mise en œuvre d'un processus de déchiffrement d'un ensemble de données chif-

frées, conformément au processus de chiffrement objet de la présente invention tel que décrit en liaison avec les figures 3a, 3b et 3c ;

- la figure 4 représente, à titre illustratif, un schéma synoptique général d'un système de sécurisation de données, conforme à l'objet de la présente invention ;

- la figure 5a représente, à titre illustratif, une structure de données particulière constituant l'enveloppe électronique signée associée à l'ensemble des données chiffrées transmises, permettant de garantir l'absence de toute attaque par rejeu du système de sécurisation de données objet de la présente invention ;

- la figure 5b représente un schéma synoptique de l'architecture logicielle d'une fonction d'anti-clonage de cartes à microprocesseur utilisées comme organe périphérique d'un ordinateur constitutif d'un système de sécurisation de données conforme à l'objet de la présente invention ;

- la figure 5c représente, à titre illustratif, un organigramme illustratif du processus d'anti-clonage de cartes à microprocesseur mis en œuvre par le noyau logiciel représenté en figure 5b, dans un mode de réalisation préférentiel du système de sécurisation de données, objet de la présente invention.

Une description plus détaillée du procédé de sécurisation de données numériques traitées par un ordinateur conforme à l'objet de la présente invention sera maintenant donnée en liaison avec les figures 1a, 1b et les figures suivantes.

D'une manière générale, on indique que l'ordinateur permettant le traitement des données et la sécurisa-

tion de ces dernières est muni d'une clé physique de protection, encore appelée *"dongle"*, cette clé physique de protection étant installée sur le port parallèle de l'ordinateur par exemple. On rappelle que ce type de clé de protection physique est un élément matériel fabriqué aux Etats-Unis par la société RAINBOW Technologies. Cet élément matériel consiste essentiellement en une mémoire programmable, comportant au moins certaines parties dont l'accès est protégé en écriture/lecture.

Cette clé physique de protection permet de délivrer à l'ordinateur un code de clé physique, noté K, ainsi que des valeurs spécifiques de paramétrage cryptographique, notées VPC, à ce dernier.

D'une manière générale, en ce qui concerne d'une part le mode opératoire de ce type de clé physique de protection, tant en ce qui concerne l'accès au code de clé physique K qu'aux valeurs spécifiques de paramétrage cryptographique VPC, on pourra utilement se reporter à la description de la demande de brevet français publiée sous le numéro 2 762 111 précédemment mentionnée dans la description et introduite dans la présente demande de brevet à titre de référence.

Ainsi que représenté sur la figure 1a, le procédé, objet de la présente invention, consiste, pour tout ensemble E de données numériques traitées par l'ordinateur, à chiffrer, en une étape 1000, cet ensemble de données E à partir d'au moins une clé de chiffrement, notée K_c, et de valeurs spécifiques de paramétrage cryptographique, notées VPC, pour engendrer un ensemble de données chiffrées, noté CE. Sur la figure 1a, l'opération consistant à chiffrer l'ensemble de données est noté par la relation :

$$CE = C_{KC}.E$$

Dans cette relation, le terme C_{KC} désigne l'opération de chiffrement proprement dite à partir de la clé de chiffrement K_c et des valeurs spécifiques de paramétrage cryptographiques VPC précédemment mentionnées. Par clé de chiffrement, on entend toute clé telle qu'une clé privée à laquelle est associée une clé publique lors de la mise en œuvre d'un processus de chiffrement/déchiffrement asymétrique à clé privée et à clé publique, ou, le cas échéant, en une clé secrète lors de la mise en œuvre d'un processus de chiffrement/déchiffrement symétrique.

L'ensemble de données chiffrées CE étant obtenu, le procédé, objet de la présente invention, consiste à associer, en une étape 1001, à l'ensemble de données chiffrées précité, une enveloppe électronique signée, notée ES, ainsi que représenté sur la figure la précitée.

L'association à l'ensemble de données chiffrées CE de l'enveloppe électronique signée ES peut être réalisée par une opération de concaténation de l'ensemble de données chiffrées CE et de l'enveloppe électronique signée ES ou, le cas échéant, par une écriture en mémoire à des adresses en mémoire adaptée, puis sauvegarde de l'ensemble.

On comprend ainsi qu'après l'opération 1001, l'ensemble formé par l'ensemble de données chiffrées CE et l'enveloppe électronique signée ES peut alors être transmis ou stocké dans des conditions de sécurité particulièrement optimales, ainsi qu'il sera décrit ultérieurement dans la description.

Ainsi qu'on l'a représenté en figure la, d'une part, mais également de manière plus détaillée en figure

1b d'autre part, l'enveloppe électronique signée ES peut comporter avantageusement des paramètres non chiffrés, tels qu'un aléa de p bits noté A, un motif d'identification d'enveloppe électronique signée, noté MI, codé par exemple sur S bits, ce motif d'identification étant calculé à partir d'au moins une des valeurs spécifiques de paramétrage cryptographique VPC, afin de permettre de vérifier l'existence d'un ensemble de données chiffrées associé à cette enveloppe électronique signée ES.

Cette dernière peut en outre comporter un numéro NK représentatif de la clé physique de protection équipant l'ordinateur et une signature électronique conjointe, notée SEC, obtenue à partir d'une signature de l'ensemble de données chiffrées et d'une signature des paramètres non chiffrés précédemment mentionnée de l'enveloppe électronique ES.

Lors de l'utilisation des données chiffrées de l'ensemble de données chiffrées CE, l'ensemble de ces paramètres non chiffrés et de la signature conjointe de l'enveloppe électronique signée permet de procéder à une vérification de l'authenticité des paramètres non chiffrés de l'enveloppe électronique signée. Cette opération peut bien entendu être effectuée par vérification de la signature conjointe précitée lors de l'utilisation, la valeur vraie de cette vérification d'authenticité de signature permettant de conclure à l'authenticité des paramètres non chiffrés précédemment mentionnés dans la description. La valeur vraie de cette vérification permet également de vérifier l'intégrité de l'ensemble des données chiffrées et des paramètres non chiffrés de l'enveloppe électronique signée. Ces vérifications d'authenticité et d'intégrité

étant effectuées, l'utilisateur peut alors procéder au déchiffrement des données chiffrées de l'ensemble des données chiffrés CE, pour utilisation. Cette opération ne peut être réalisée que dans la mesure où l'utilisateur détient à la fois les droits d'accès et d'usage des prestations cryptographiques proposées par le processus de sécurisation des données.

Bien entendu, le procédé de sécurisation de données numériques traitées par un ordinateur, objet de la présente invention, s'applique à la sécurisation de données en mode local, cette sécurisation étant réalisée sur des données traitées par une station de travail par exemple, puis, suite à l'obtention des données sécurisées, à un stockage de ces données sur un support de mémorisation en vue d'un archivage et/ou d'une transmission du support, ainsi que mentionné précédemment par exemple.

Il trouve également application à la sécurisation de ces mêmes données au niveau d'une station de travail et à la transmission des données sécurisées sur un réseau de transmission. Dans ce cas, le mode de sécurisation est dit distant, dans la mesure où le procédé, objet de la présente invention, permet de bénéficier de la sécurisation de l'ensemble des données et de leur transmission dans les conditions qui seront décrites ci-après.

Dans ce but, les paramètres non chiffrés de l'enveloppe électronique signée ES peuvent comporter avantageusement, ainsi que représenté en figure 1b, en outre, un bit U indicateur du mode d'utilisation local monoposte au niveau de l'ordinateur ou du mode d'utilisation distant en réseau multipostes de ces données chiffrées.

Alors que lors de l'utilisation monoposte du procédé, objet de la présente invention, le bit indicateur du mode d'utilisation local auquel a été affectée une valeur donnée pourrait être jugé comme non significatif pour la mise en œuvre du procédé selon l'invention, ce dernier au contraire prend en compte la valeur de ce bit pour effectuer le calcul de la signature conjointe à partir des paramètres non chiffrés, ainsi que mentionné précédemment dans la description.

De même, pour une mise en œuvre et une utilisation du procédé, objet de la présente invention, en mode distant, les paramètres non chiffrés de l'enveloppe électronique signée ES peuvent avantageusement comporter, ainsi que représenté en figure 1b, un code détecteur/correcteur d'erreurs, noté CRC, permettant après transmission une vérification de l'intégrité des données chiffrées et signées transmises.

Dans un mode de réalisation particulier non limitatif, on indique que le code détecteur/correcteur d'erreurs utilisé était un code BCH(255,215,11) avec le paramètre t=5, dont la redondance ou CRC est de 40 bits. D'une manière générale, on indique que le champ contenant le code détecteur/correcteur d'erreurs peut être placé, de préférence, en une position quelconque dans l'enveloppe électronique signée ES.

En outre, ainsi que représenté également en figure 1b, pour une utilisation ou une mise en œuvre du procédé, objet de l'invention en mode distant, les paramètres non chiffrés de l'enveloppe électronique signée ES comportent avantageusement un code d'identification de l'expéditeur, noté ME, de l'ensemble de données chiffrées CE, afin de

permettre de procéder à une vérification de non-répudiation de cet expéditeur.

De même, en référence à la figure 1b, on indique que, pour une mise en œuvre et une utilisation du procédé, objet de la présente invention, en mode distant, les paramètres non chiffrés peuvent comporter en outre un code d'identification du destinataire de cet ensemble de données chiffrées, code noté MD sur la figure 1b. L'existence de ce code permet d'assurer un acheminement sélectif des données chiffrées en fonction du code d'identification du destinataire ainsi que des droits attribués à ce dernier. Dans ce cas, l'opération de déchiffrement des données chiffrées par le destinataire, alors que l'ensemble des tests de vérification d'authenticité et d'intégrité des données a été satisfait, permet de prouver la validité de l'acheminement sélectif précédemment mentionné dans les conditions de respect des droits alloués au destinataire considéré. Bien entendu, ces droits s'entendent pour ce dernier en l'autorisation de procéder à des opérations de chiffrement/déchiffrement, de signature/vérification de signature et de vérification de la validité de la période d'abonnement par exemple. Ces droits peuvent être attribués au destinataire en fonction de critères légaux en vigueur dans le pays d'utilisation.

Enfin, les paramètres non chiffrés de l'enveloppe électronique signée ES peuvent comporter en outre une valeur de date temps réel de l'opération de chiffrement.

Dans un mode de réalisation particulier non limitatif, on indique que le format global de l'enveloppe électronique signée ES était de 32 octets, le code détec-

teur/correcteur d'erreurs BCH(255,215,11) ayant été utilisé en détection d'erreurs.

Dans ce mode de réalisation, l'enveloppe électronique ES comportait :

- l'aléa A de 4 bits,
- le bit indicateur U du mode local ou distant utilisé,
- le motif d'identification MI, codé sur 31 bits,
- le motif d'identification ME de l'expéditeur, codé sur 16 bits,
- le motif d'identification MD du destinataire, codé sur 16 bits,
- le numéro apparent NK de la clé physique de protection, codé sur 16 bits,
- la date de chiffrement, notée DATE, codée sur 35 bits et correspondant à une date exprimée en année, mois, jour, heure, minute et seconde,
- la signature conjointe, notée SEC, codée sur 64 bits,
- le code détecteur/correcteur d'erreurs, avec une redondance codée sur 40 bits, tel que mentionné précédemment,
- et enfin, la ou les fonctions cryptographiques FA allouées à l'expéditeur et auxquelles il a droit d'usage, codées sur 14 bits.

Un champ relatif à un code lié aux valeurs spécifiques de paramétrage cryptographique VPC peut en outre être prévu. Dans le cas où ces valeurs spécifiques VPC sont mémorisées sur un support externe, tel qu'une carte électronique ou carte à microprocesseur, le champ précité

peut comporter le numéro physique NPC de la carte à microprocesseur de l'expéditeur.

Compte tenu de l'ensemble des paramètres non chiffrés et de la signature électronique conjointe SEC précédemment mentionnée, le procédé, objet de la présente invention, fournit des services cryptographiques recouvrant l'ensemble des prestations cryptographiques, à savoir :

- confidentialité des données transmises, l'ensemble des données pouvant être chiffré ou déchiffré à volonté de manière sécurisée,

- distribution des clés, l'ensemble des clés et les données sensibles ainsi que les paramètres nécessaires au bon fonctionnement des prestations cryptographiques sont distribués sur des supports physiques tels que le "*dongle*" et une carte à microprocesseur ainsi qu'il sera décrit ultérieurement dans la description ;

- authentification : cette authentification est réalisée par l'intermédiaire de l'enveloppe électronique signée ES jointe par l'expéditeur de l'ensemble des données chiffrées CE, le destinataire ayant ainsi la possibilité de vérifier l'authenticité des éléments actifs de l'enveloppe électronique, c'est-à-dire des paramètres non chiffrés ;

- intégrité de premier niveau : l'intégrité de premier niveau étant obtenue du fait de la prise en charge par un code détecteur/correcteur d'erreurs BCH(255,215,11) précédemment cité, avec le paramètre t=5, ce code permettant de détecter les erreurs de transmission de l'ensemble des données chiffrées transmises ;

- intégrité de deuxième niveau :la signature conjointe permet de s'assurer de l'intégrité du fichier informatique chiffré et de l'enveloppe électronique ;

- répudiation/non-répudiation, la non-répudiation de l'expéditeur étant obtenue du fait de l'enveloppe électronique signée ES munie du champ d'identification de l'expéditeur ME, lequel sert donc de preuve à la non-répudiation.

En ce qui concerne la distribution sélective de l'ensemble des données chiffrées CE, on indique que celle-ci est obtenue du fait de la vérification du code destinataire MD et de l'enveloppe électronique signée ES, le déchiffrement servant bien entendu de preuve à la valeur vraie de la distribution sélective précitée dans les conditions de droit d'accès définies précédemment.

Enfin, on remarquera que l'enveloppe électronique signée ES est unique, la date et l'heure du chiffrement, l'édition de journal de bord en cas de succès des prestations cryptographiques sollicitées permettant de retracer l'historique des opérations et de prendre les mesures correctives si besoin est.

Une description plus détaillée du mode opératoire mis en œuvre afin de calculer la signature électronique conjointe précédemment citée sera maintenant donnée en liaison avec les figures 2a et 2b.

D'une manière générale, on indique que le calcul de la signature électronique conjointe SEC doit être effectuée à partir des données chiffrées, c'est-à-dire de l'ensemble CE, et des paramètres non chiffrés de l'enveloppe électronique signée ES, ces paramètres non chiffrés étant notés par commodité $\overline{ES}$, cette notation étant justi-

fiée par le fait que les paramètres non chiffrés sont en fait complétés par la valeur de signature conjointe calculée pour constituer l'enveloppe électronique signée ES considérée.

Pour calculer la valeur de signature électronique conjointe, notée SEC, il est donc nécessaire de partir de l'ensemble de données chiffrées CE ainsi que des paramètres non chiffrés $\overline{ES}$ de l'enveloppe électronique ES.

A partir de ces éléments précités, le procédé, objet de la présente invention, ainsi que représenté en figure 2a, consiste, pour calculer la signature électronique conjointe, en une opération de signature comprenant une étape 3000 consistant à calculer une signature externe sur n octets de l'ensemble de données chiffrées CE à partir de ressources cryptographiques auxiliaires à l'ordinateur précédemment cité. Sur la figure 2a, l'opération de calcul d'une signature externe sur n octets est notée selon la relation :

$$SE = S_x.CE$$

Dans cette relation, x désigne une clé de signature spécifique à la mise en œuvre de l'opération 3000 représentée en figure 2a et S_x désigne l'opération de calcul de signature sur l'ensemble des données chiffrées CE. Suite à l'opération 3000, on obtient la valeur de signature externe, notée SE, codée sur n octets de l'ensemble des données chiffrées précité.

L'opération de calcul de la signature électronique conjointe consiste en outre, ainsi que représenté en 3001, à calculer une signature interne sur n octets, cette signature étant calculée à partir des paramètres non chif-

frés $\overline{ES}$ de l'enveloppe électronique signée ES à partir d'un processus cryptographique à clé secrète.

A l'étape 3001 de la figure 2a, l'opération de signature interne est désignée par la relation :

$$S_{ES} = S_{DES}.\overline{ES}.$$

Dans la relation précitée, S_{ES} désigne la valeur de signature interne calculée sur n octets des paramètres non chiffrés de l'enveloppe électronique, S_{DES} désigne un processus de calcul de signature à clé secrète.

Dans un mode de réalisation particulier non limitatif, on indique que le processus cryptographique de calcul de signature à clé secrète était le processus DES. Le processus de chiffrement à partir de l'algorithme DES est satisfaisant car les clés de chiffrement autorisées par les pouvoirs publics dans les différents états souverains ont récemment été portées à des valeurs permettant d'assurer une confidentialité satisfaisante.

En outre, ainsi que représenté en figure 2a, les opérations 3000 et 3001 sont suivies d'une opération 3002 consistant à effectuer une opération de combinaison logique OU exclusif bit à bit entre la signature externe SE et la signature interne S_{ES}. On dispose à la fin de l'étape 3002 de la signature électronique conjointe notée SEC.

Un mode de réalisation non limitatif du procédé de calcul de signature électronique conjointe décrit précédemment en figure 2a sera maintenant donné en liaison avec la figure 2b.

Ce mode de réalisation peut être mis en œuvre en particulier lorsque le micro-ordinateur, outre le *"dongle"*

précédemment mentionné, est équipé d'un lecteur de carte à microprocesseur, l'utilisateur habilité disposant d'une telle carte à microprocesseur.

Dans ce cas, ainsi que représenté en figure 2b, l'étape 3000 de la figure 2a peut être réalisée de la manière ci-après. En une étape 3000a, à partir de l'ensemble des données chiffrées CE, un processus de diversification ou de brassage de ces données chiffrées peut être réalisé par découpage de ces données en chaînes de 28 bits successives, et brassage selon une loi appropriée de l'ensemble des chaînes successives ainsi réalisées. Le brassage est représenté par la croix cerclée en figure 2b. L'ensemble des données chiffrées diversifiées est noté CE* en figure 2b.

A partir d'une clé de chiffrement x, l'étape 3000 peut être alors mise en œuvre à partir des données brassées CE* et de l'adresse absolue de la carte à microprocesseur à l'étape 3000b par une opération de signature de type *TELEPASS* à l'étape 3000c. On obtient ainsi, en fin d'étape 3000c, la signature externe SE déjà mentionnée en figure 2a.

De même, l'étape 3001 peut être réalisée par l'application à partir d'une clé secrète de chiffrement K_S de l'algorithme de chiffrement DES, opération notée S_{DES} dans le bloc 3001 de la figure 2b, à l'ensemble des paramètres non chiffrés $\overline{ES}$ de l'enveloppe électronique signée ES.

L'opération OU exclusif appliquée à la signature externe SE et à la signature interne S_{ES} obtenue à l'étape 3001 permet alors d'obtenir la signature électronique conjointe SEC.

Bien entendu, au niveau de l'utilisation, pour réaliser la vérification de signature de la signature électronique conjointe SEC, il est nécessaire, à partir de la valeur calculée de la signature interne S_{ES} par application de la clé secrète K_S et de l'algorithme DES aux paramètres non chiffrés $\overline{ES}$, de calculer par combinaison de type OU exclusif appliquée à la signature électronique conjointe SEC, la valeur de la signature externe SE, puis par un processus symétrique de vérification de signature télé-pass, d'authentifier la valeur de l'ensemble des données chiffrées CE transmis au destinataire.

Une description plus détaillée d'un mode opératoire préférentiel mis en œuvre pour assurer le chiffrement de données E pour engendrer l'ensemble de données chiffrées CE sera maintenant décrit en liaison avec les figures 3a à 3d.

En référence à la figure 3a, on indique que l'opération de chiffrement précitée consiste essentiellement, à partir de l'ensemble des données E, à engendrer par calcul une suite chiffrante à partir d'un générateur pseudo-aléatoire, cette suite chiffrante constituant la clé de chiffrement notée K_c.

D'une manière générale, on indique que la clé de chiffrement est maintenue secrète, c'est-à-dire que cette clé de chiffrement est calculée instantanément au niveau de l'ordinateur, mais qu'elle n'est pas accessible directement à l'utilisateur. Le mode opératoire utilisé pour engendrer la suite chiffrante sera décrit ultérieurement dans la description.

Suite à l'obtention de la suite chiffrante K_c à l'étape 4000, le procédé, objet de l'invention, pour assu-

rer le chiffrement de l'ensemble des données E, consiste alors, en une étape 4001, à effectuer une combinaison logique de type OU exclusif d'octet à octet entre l'ensemble de données E et la suite chiffrante K_c de manière à engendrer l'ensemble de données chiffrées CE. Sur la figure 3a, l'opération de combinaison logique OU exclusif est notée selon la relation :

$$CE = XOR(E, K_c)$$

A la fin de l'étape 4001, on dispose de l'ensemble des données chiffrées CE.

Un exemple de mise en œuvre préférentielle non limitatif de l'opération de calcul de la suite chiffrante sera maintenant donnée en liaison avec la figure 3b, un mode de réalisation correspondant d'un processus de chiffrement de l'ensemble de données E pour engendrer un ensemble de données chiffrées CE étant donné en figure 3c.

En référence à la figure 3b, on indique que l'étape consistant à engendrer la suite chiffrante peut consister avantageusement en une étape 5000, à choisir dans l'ensemble de données numériques E, c'est-à-dire préalablement à l'opération de chiffrement, un premier et un deuxième mot, notés respectivement A, B. D'une manière générale, on indique que chaque mot A, B peut être un mot de q octets avec q=3 octets par exemple.

L'étape consistant à engendrer la suite chiffrante consiste en outre à sélectionner un premier E_a et un deuxième E_b mot de référence de même taille en nombre d'octets, c'est-à-dire de même taille égale à q octets que celle du premier et du deuxième mot A, B, respectivement.

D'une manière générale, on indique que les premier E_a et les deuxième E_b mots de référence, lorsque l'ordinateur est équipé d'un lecteur de carte à microprocesseur et d'une carte à microprocesseur dédiée à l'utilisateur, peuvent être sélectionnés parmi les données de la carte à microprocesseur.

En outre, dans un mode de réalisation spécifique, les mots A et B peuvent être soumis à une étape de diversification, notée 5002, laquelle consiste à partir de ces mots A et B à obtenir des mots diversifiés, notés A*, respectivement B*. Ces mots diversifiés sont obtenus par une opération de brassage des bits constitutifs des octets dans des conditions qui seront décrites de manière plus détaillée ultérieurement dans la description.

Lorsque l'opération de diversification 5002 n'est pas réalisée, on indique que A = A* et que B = B*.

Pour la suite de la description, le procédé, objet de la présente invention, sera décrit en considérant la mise en œuvre des mots diversifiés A* et B*, lesquels, dans le cas particulier précédemment cité de l'absence de diversification, reviennent à substituer A à A* et B à B*.

Ainsi, l'étape consistant à engendrer la suite chiffrante consiste alors, en une étape 5003, à former par combinaison logique de type OU exclusif, octet à octet, une valeur égale à la combinaison logique du premier mot et du premier mot de référence, ainsi que du deuxième mot et du deuxième mot de référence pour obtenir une première et une deuxième clé virtuelle, notées KV_1 et KV_2.

Sur la figure 3b, l'étape 5003 est définie par les relations :

$$KV_1 = XOR(A^*, E_a)$$

et

$$KV_2 = XOR(B^*, E_b)$$

La suite chiffrante K_c correspondant à la clé de chiffrement est ensuite engendrée à l'étape 5004 à partir des clés virtuelles et de polynômes générateurs, l'opération correspondante étant notée à l'étape 5004 selon la relation :

$$K_c = f(KV_1, KV_2)$$

et réalisée dans des conditions qui seront décrites ci-après dans la description.

Les mots A et B de q octets, avec q=3 par exemple, sélectionnés dans l'ensemble des données E non chiffrées, permettent de garantir l'irréversibilité du processus de chiffrement. Les mots A et B peuvent subir l'opération de diversification, c'est-à-dire de brassage pour engendrer les mots A* et B*, grâce à une opération de rotation circulaire et une addition modulo 2 par exemple.

L'opération 5003 correspond à une addition modulo 2 avec le premier et le deuxième mot de référence E_a, E_b, lesquels sont lus dans la carte à microprocesseur à l'étape 5001.

Dans un mode de réalisation spécifique, les mots E_a et E_b forment une liste de 10 valeurs.

Ainsi, le choix de la valeur utilisée peut dépendre de la taille du fichier représentatif de l'ensemble des données E à soumettre au processus de chiffrement.

De la même manière, les positions respectives des mots A et B dans l'ensemble de données E à soumettre au

chiffrement dépendent de la taille du fichier représentatif de cet ensemble E.

Dans un exemple de réalisation, la taille de 11 020 octets d'un fichier informatique représentatif de l'ensemble E est utilisée comme paramètre principal pour la mise en œuvre du procédé.

Mot A :

Le mot A peut être constitué de 3 octets, a_1, a_2 et a_3, dont la position dépend de la taille du fichier. A titre d'exemple, a_1, a_2 et $a_3 \in \{0,1,2,\ldots, 255\}$.

L'adresse de l'octet a_1 peut être prise égale à la taille du fichier divisée par un diviseur D_1 et en particulier à la valeur entière de cette division. Les adresses des octets a_2 et a_3 peuvent être obtenues en ajoutant respectivement les valeurs 1 et 2 à celle de l'octet a_1. Les valeurs du diviseur D_1 sont données à titre d'exemple non limitatif en fonction de la taille du fichier à chiffrer en octets dans le tableau 1 ci-après.

TABLEAU 1

Taille du fichier à chiffrer en octets	]16,4095[	[4095,16384[	[16384,65536[	[65536,∞[
Diviseur D_1	7	121	137	253

Le mot A peut alors être soumis à un décalage de y bits à droite, la valeur de décalage y étant obtenue par la valeur de décalage z augmentée de la valeur 2 modulo 24. La valeur de décalage z est définie plus loin.

Mot B :

Le mot B est constitué de 3 octets, b_1, b_2 et b_3, et la position de ces octets dépend de la taille du fichier représentatif de l'ensemble E. A titre d'exemple, b_1, b_2 et b_3 $\in \{0,1,2,\ldots,255\}$.

L'adresse de l'octet b_1 peut être prise égale à la taille du fichier divisée par le diviseur D_2, la valeur entière du résultat de la division étant seule prise en compte. Les adresses des octets b_2 et b_3 peuvent alors être obtenues en ajoutant respectivement les valeurs 1 et 2 à celle de l'octet b_1. La valeur du diviseur D_2, en fonction de la taille du fichier représentatif de l'ensemble E, est donnée dans le tableau 2 ci-après.

TABLEAU 2

Taille du fichier à chiffrer en octets	]16,4095[	[4095,16384[	[16384,65536[	[65536,∞[
Diviseur D_2	3	11	13	19

Le mot B peut alors être soumis à un décalage de z bits à gauche, z étant défini par la taille du fichier modulo 24.

Mots de référence E_a et E_b :

Une liste des mots de référence E_a et E_b utilisés et leurs indices respectifs I_a et I_b est mémorisée dans la mémoire à accès protégé de la carte à microprocesseur dédiée à l'utilisateur. A chaque indice I_a et I_b est allouée une

valeur arbitraire correspondant au mot de référence E_a, respectivement E_b.

Le mot E_a utilisé est lu dans la mémoire protégée et désigné par son indice I_a, l'indice I_a étant obtenu par exemple par la valeur de la taille du fichier représentatif de l'ensemble E modulo 5.

Le mot E_b est désigné par son indice I_b, l'indice I_b étant obtenu à partir d'une formule liant les indices I_a et I_b selon la relation :

$$I_b = [(I_a+2) \bmod 5]+5$$

Polynômes générateurs p(x) :

La liste des polynômes générateurs précités utilisés, ainsi que la représentation de ces polynômes en valeur hexadécimale est mémorisée dans la mémoire à accès protégé.

Le polynôme générateur p(x) utilisé par le générateur pseudo-aléatoire est désigné par son numéro. Ce numéro peut être pris égal à la somme de la taille du fichier représentatif de l'ensemble E et des mots A et B modulo 10.

A titre d'exemple de référence, les registres à décalage du polynôme générateur sont initialisés à la valeur initiale en hexadécimal B084 pour des tailles de fichiers représentatifs d'ensembles de données E à chiffrer dépassant la longueur maximale.

Le numéro du polynôme générateur utilisé correspondant à une valeur donnée, 6 par exemple, permet d'appeler la valeur du polynôme représenté en valeur hexadécimale sous la forme :

- forme hexadécimale : p(x) = 103DD

- forme polynomiale : $p(x) = X^{16}+X^9+X^8+X^7+X^6+X^4+X^3+X^2+1$.

Les valeurs de mots A, mot de référence E_a, indice I_a, et des valeurs de clé virtuelle KV_1, respectivement mot B; mot de référence E_b, indice I_b et clé virtuelle KV_2 sont données dans les tableaux 3 et 4 ci-après :

TABLEAU 3

	Mot A Octet a_1	Octet a_2	Octet a_3	Mot E_a	Indice I_a	Mot A modifié ou clé virtuelle
Adresse	005B	005C	005D			
Valeurs	68	65	63	8B4BC0	0	06EA55

TABLEAU 4

	Mot B Octet b_1	Octet b_2	Octet b_3	Mot E_b	Indice I_b	Mot B Modifié ou clé virtuelle
Adresse	03E9	03EA	03EB			
Valeurs	59	54	45	DD595E	7	481D08

Une description plus détaillée d'un mode de mise en œuvre préférentiel de l'opération de chiffrement de l'ensemble E des données numériques sera maintenant donnée en liaison avec la figure 3c en référence aux figures 3a et 3b précédentes.

D'une manière générale, l'opération de chiffrement précitée est réalisée à partir de la suite chiffrante, notée K_c, obtenue par exemple suite à l'étape 5004 de la figure 3b.

Conformément au mode de réalisation préférentiel précité, l'opération de chiffrement peut consister, ainsi que représenté en figure 3c, en une étape 5005, à remplacer les premier A et deuxième B mots de l'ensemble E de données numériques par la première, respectivement la deuxième clé virtuelle KV_1, KV_2, pour engendrer un ensemble de données numériques incrusté, noté E'. Cette opération peut être effectuée par des opérations classiques de pointage en mémoire des mots A, B et de réinscription à l'adresse correspondante des clés virtuelles KV_1 et KV_2.

Suite à l'étape 5005 précitée, l'opération de chiffrement consiste alors à soumettre à un processus de chiffrement l'ensemble des données numériques incrustées E' à l'exception des première et deuxième clés virtuelles incrustées KV_1 et KV_2 pour engendrer l'ensemble de données chiffrées CE.

L'opération de chiffrement correspondante à l'étape 5006 est notée selon la relation :

$$CE = XOR(E', K_c) \text{ sauf } KV_1, KV_2.$$

Ainsi, l'opération de chiffrement à l'étape 5006 correspond à celle représentée en figure 3a à l'étape 4001 sauf pour les clés virtuelles incrustées KV_1 et KV_2. Une telle opération peut être réalisée par lecture séquentielle des octets successifs constitutifs de l'ensemble des données à chiffrer E, discrimination du rang de chaque octet, chiffrement des octets dont le rang ne correspond pas au rang des octets constitutifs des clés virtuelles incrustées KV_1 et KV_2 et absence de chiffrement des octets

de rang correspondant aux octets constitutifs des clés virtuelles KV_1 et KV_2.

Un processus de déchiffrement des données chiffrées, c'est-à-dire de l'ensemble de données chiffrées E' obtenu grâce à la mise en œuvre du processus de chiffrement tel que représenté en figure 3c, sera maintenant décrit en liaison avec la figure 3d.

Ainsi que représenté sur la figure précitée, lors de l'utilisation, le processus de déchiffrement peut consister, en une étape 6000, à discriminer dans l'ensemble de données chiffrées CE les première et deuxième clés virtuelles incrustées KV_1 et KV_2. Cette discrimination est réalisée à partir de la lecture à l'adresse correspondante des octets constitutifs des clés virtuelles KV_1 et KV_2.

En outre, le processus de déchiffrement consiste également, à partir d'une lecture des données de la carte à microprocesseur permettant de restituer les mots de référence E_a et E_b, cette lecture étant effectuée à partir des indices I_a et I_b précédemment mentionnés dans la description, cette étape de lecture étant réalisée à l'étape 6001 de la figure 3b, à restituer, par combinaison logique de type OU exclusif à une étape 6002, les premier A et deuxième B mots à partir des clés virtuelles incrustées KV_1 et KV_2.

Sur la figure 3d, on a représenté l'opération réalisée à l'étape 6002 pour un premier mot A et un deuxième mot B correspondant en fait à des mots diversifiés A* et B* ainsi que mentionné précédemment dans la description. Dans ces conditions, lorsqu'aucune diversification des premier et deuxième mots A, B n'a été effectuée, ainsi que représenté en 6002a en figure 3d, au premier mot A* cor-

respond le mot A et au deuxième mot B* correspond le deuxième mot B.

Le processus de déchiffrement peut alors ensuite consister à remplacer dans les données chiffrées de l'ensemble de données chiffrées CE les clés virtuelles KV_1 et KV_2 par le premier A, respectivement le deuxième mot B. Ceci permet de restituer un ensemble de données numériques chiffrées modifiées, noté CE'.

L'étape 6002b de remplacement peut alors être suivie d'une étape 6003 consistant à restituer à partir des clés virtuelles la suite chiffrante. Cette opération est notée sur la figure 3d selon la relation :

$$K_c = f(K_{v1}, K_{v2})$$

et correspond à celle précédemment décrite dans la description à la figure 3b à l'étape 5004.

D'une manière générale, on indique que les étapes 6002b et 6003 peuvent être interverties sans inconvénient. Il en est de même pour les étapes 6000 et 6001 précédentes.

Enfin, le processus de déchiffrement représenté en figure 3b consiste, à l'étape 6004, à soumettre l'ensemble de données numériques chiffrées modifiées CE' à un processus de déchiffrement proprement dit à partir de la suite chiffrante K_c obtenue à l'étape 6003 précédente à l'exception des premier et deuxième mots A, B. Ceci permet de restituer les données numériques de l'ensemble de données numériques pour utilisation. Cette opération est notée à l'étape 6004 selon la relation :

$$E = XOR(CE', K_c) \text{ sauf A, B.}$$

On rappelle que l'opération de déchiffrement à l'étape 6004 est l'opération duale de l'opération de chiffrement à l'étape 5006 de la figure 3c.

Un système de sécurisation de données numériques traitées par un ordinateur, conforme à l'objet de la présente invention, sera maintenant décrit en liaison avec la figure 4 et les figures suivantes.

Sur la figure précitée, on indique que l'ordinateur 1 est muni d'une clé physique de protection 2, laquelle délivre à ce dernier un code de clé physique K et des valeurs spécifiques de paramétrage cryptographique notées VPC précédemment dans la description en liaison avec la figure 1b.

Le système, objet de la présente invention, comporte également un module de chiffrement de l'ensemble des données à chiffrer E à partir d'au moins une clé de chiffrement K_c pour engendrer l'ensemble de données chiffrées CE précédemment mentionné dans la description. Le module de chiffrement précité correspond à un module logiciel, la clé de chiffrement K_c correspondant à la suite chiffrante et l'opération de chiffrement par ce module logiciel étant réalisée conformément au processus de chiffrement précédemment décrit dans la description en liaison avec les figures 3a, 3b et 3c.

Le système, objet de la présente invention, comporte également un module de calcul à partir de l'ensemble de données chiffrées CE de l'enveloppe électronique signée ES telle que décrite en liaison avec les figures 1a ou 1b précédemment dans la description.

Le module de calcul de l'enveloppe électronique signée ES est bien entendu réalisé par un module logiciel,

lequel, à partir des variables d'état délivrées par le système d'exploitation de l'ordinateur et des paramètres de configuration de ce dernier, permet d'instancier la valeur des champs de l'enveloppe électronique signée ES et de concaténer l'ensemble des champs précités pour construire et mémoriser l'enveloppe électronique signée ES telle que représentée en figure 1a ou 1b par exemple. La concaténation de l'enveloppe signée ES et de l'ensemble des données chiffrées CE est réalisée de manière semblable. Ces opérations de type classique sont connues en tant que telles et, pour cette raison, ne seront pas décrites en détail. Ainsi, les données sécurisées sont constituées par la concaténation de l'enveloppe électronique signée ES et de l'ensemble des données chiffrées CE.

D'une manière générale, on indique que le système, objet de la présente invention, comporte en outre un module générateur de la suite chiffrante intégré au module de chiffrement de l'ensemble des données E, ainsi qu'un module de combinaison logique OU exclusif d'octet à octet pour engendrer l'ensemble de données chiffrées à partir de la suite chiffrante et de l'ensemble de données E. Le module de chiffrement est un module logiciel permettant la mise en œuvre du procédé, objet de la présente invention tel que représenté en figures 3a et 3b, 3c par exemple.

Le système, objet de la présente invention, tel que représenté en figure 4, comprend également un module de calcul de l'enveloppe électronique signée ES, lequel peut être configuré en un module de calcul de signature externe sur n octets de l'ensemble de données chiffrées à partir de ressources cryptographiques auxiliaires externes à l'ordinateur et en un module de calcul de signature in-

terne sur n octets des paramètres non chiffrés $\overline{ES}$ de l'enveloppe électronique ES à partir d'un processus cryptographique à clé secrète. Le module de calcul de la signature électronique conjointe SEC est un module logiciel permettant la mise en œuvre du processus de calcul précédemment décrit en liaison avec les figures 2a ou 2b.

Ainsi que représenté sur la figure 4, à l'ordinateur 1 constitutif du système, objet de la présente invention, est en outre associé un ensemble constitué par une carte à microprocesseur munie de ressources cryptographiques et une interface de carte à microprocesseur connectée à l'ordinateur 1. La carte à microprocesseur est munie de ressources cryptographiques afin de constituer les ressources cryptographiques auxiliaires précédemment mentionnées dans la description.

Dans un mode de réalisation préférentiel non limitatif, le lecteur de carte à microprocesseur était un lecteur de type TLP 224 NV2 commercialisé en France par la société BULL, et la carte à microprocesseur utilisée était une carte à microprocesseur personnalisée de type SCOT. En outre, on indique que l'ensemble lecteur de carte à microprocesseur / carte à microprocesseur peut être remplacé par une interface de type PCMCIA commercialisée sous la dénomination *SecurLINK II* par la société BULL utilisant la même carte à microprocesseur.

Le mode opératoire fonctionnel du système, objet de la présente invention, ainsi constitué, est alors le suivant :

Le système, objet de la présente invention, utilise en fait deux technologies distinctes afin de permet-

tre un renforcement mutuel du niveau de sécurité offert par chacune d'elles.

La carte à microprocesseur et la clé de protection physique ou *"dongle"* échangent en permanence des données sensibles selon un protocole interactif et contribuent ainsi à durcir le système et à augmenter le niveau global de sécurité de ce dernier.

Ainsi, le système objet de la présente invention met en œuvre une sécurité répartie sur plusieurs systèmes de sécurité.

En ce qui concerne la carte à microprocesseur, on indique que l'accès aux données de cette dernière est autorisé uniquement lors de la saisie du code confidentiel associé à celle-ci. L'historique et la gestion des codes confidentiels erronés sont pris en charge par le masque de la carte à microprocesseur. Le masque de la carte à microprocesseur contrôle et valide la suite des opérations. La carte à microprocesseur contient un code d'en-tête et des données permettant de lancer le fonctionnement du générateur pseudo-aléatoire. Les polynômes générateurs p(x) de degré 16 dans leur représentation hexadécimale, les clés électroniques, les mots de référence E_a et E_b de trois octets chacun ainsi que les indices I_a et I_b les désignant font partie des données.

Le code d'en-tête et les données précités sont soumis à un processus de signature par l'algorithme cryptographique *TELEPASS* de la carte à microprocesseur. Les clés internes de l'algorithme cryptographique *TELEPASS* sont utilisées sélectivement afin d'assurer la vérification de la signature du code d'en-tête et de celle des données.

Le code d'en-tête peut être constitué par plusieurs champs de bits permettant :

- d'identifier le numéro de la carte à microprocesseur ;
- d'identifier le code d'identification de l'utilisateur ;
- d'inscrire le numéro du masque de diversification ;
- d'inscrire le seuil minimal de la taille du fichier représentatif de l'ensemble des données E à chiffrer ;
- de choisir une liste parmi deux des polynômes générateurs p(x),
- d'indiquer le type d'application ;
- d'inscrire les droits correspondants aux prestations cryptographiques autorisées, notamment date de validité, droit d'accès et d'usage ;
- d'indiquer la clé utilisée pour vérifier l'intégrité du code d'en-tête et de celle des données ;
- de trouver l'adresse absolue et l'offset des mots de référence E_a et E_b.

La clé physique de protection 2 contrôle en fait en permanence l'ensemble du système et le processus de sécurisation des données. Pour une description plus complète de ce mode de protection et du processus d'encapsulation de la fonction de sécurisation des données à partir du code de clé physique K délivré par la clé physique de protection 2, on pourra utilement se reporter à la demande de brevet français publiée sous le n° 2 762 111 précédemment mentionnée dans la description.

D'une manière générale, on indique que bien entendu, le système objet de la présente invention ne peut être utilisé lors de l'installation d'une clé physique de protection non dédiée au système objet de la présente invention et en particulier à l'ordinateur incorporant ce dernier. De même, l'usage du système, objet de la présente invention, est inhibé pour un nombre d'utilisations épuisé, lors du dépassement d'une date limite périmée ou d'un crédit en temps totalement consommé.

Les fonctionnalités précitées sont programmées par programmation de valeurs limites correspondantes dans la mémoire de la clé physique de protection considérée.

La clé physique de protection comporte en mémoire à accès protégé, d'une part, les masques de diversification de la carte à microprocesseur, et d'autre part, les paramètres dynamiques nécessaires au calcul du motif d'identification MI. On rappelle que ce motif d'identification MI est inséré dans l'enveloppe électronique signée ES.

Le système, objet de la présente invention, est ainsi protégé contre le piratage et l'utilisation illicites de ce dernier par l'intermédiaire de la clé physique de protection. Ainsi, chaque système conforme à l'objet de la présente invention est encapsulé par l'intermédiaire de paramètres spécifiques de la clé physique de protection dédiée au système considéré, c'est-à-dire à l'ordinateur hôte 1 incorporant ce système. Les critères d'encapsulation utilisés sont, d'une part, la reconnaissance algorithmique de la clé physique de protection dédiée par le noyau logiciel incorporant ce système, deux mots de 16 bits non signés sont mémorisés dans la clé physique de

protection, et, d'autre part, une encapsulation temporelle relative à l'utilisation de l'ensemble du système par l'intermédiaire de bornes de contrôle temporelles permettant d'effectuer un choix entre date limite d'utilisation ou crédit de temps alloué au système considéré.

Ainsi, la clé physique de protection est organisée de façon à pouvoir modifier des mots ou valeurs mémorisés dans cette clé physique de protection par l'intermédiaire de son numéro apparent. D'une manière générale, on indique que l'organisation consiste à prévoir une base de données, le pointage par le numéro apparent de cette base de données permettant :

- de dupliquer la clé physique de protection correspondante, c'est-à-dire les données mémorisées dans cette clé physique de protection,

- de recréer localement une clé physique de protection afin d'autoriser la mise en œuvre de l'encapsulation d'une nouvelle version du logiciel incorporant le système objet de l'invention ;

- de suivre l'historique et le cycle d'utilisation d'une clé physique de protection déterminée ;

- de procéder à l'encapsulation du logiciel précité afin de modifier les mots mémorisés dans une clé physique installée chez un utilisateur et ce, compte tenu de la reconnaissance exclusive et algorithmique de cette clé physique de protection.

Ainsi, et compte tenu de l'ensemble des opérations susceptibles d'être exécutées, il est possible d'agir à distance et de manière sélective sur les bornes de contrôle et les bornes temporelles d'une clé physique de protection installée chez un usager.

La protection du système objet de la présente invention à l'encontre d'accès illicite et en conséquence d'utilisation abusive au processus de sécurisation des données par des tiers non habilités peut en outre être sensiblement améliorée grâce à la mise en œuvre de dispositions d'inhibition d'attaque par rejeu de ce système et d'anti-clonage des cartes à microprocesseur, le cas échéant de l'interface PCMCIA et cartes à microprocesseur utilisées pour la mise en œuvre de ce système, ces dispositions étant décrites ci-après en liaison avec les figures 5a, respectivement 5b et 5c.

Afin d'inhiber toute attaque par rejeu du système objet de la présente invention par un utilisateur non habilité ayant procédé à une ou plusieurs recopies de transactions entre les ressources cryptographiques auxiliaires externes à l'ordinateur, c'est-à-dire entre l'ensemble constitué par la carte à microprocesseur et le lecteur de carte à microprocesseur 3, 3a représentés en figure 4, et l'ordinateur 1, ce type d'attaque par rejeu pouvant être conduit par un simple couplage électromagnétique au niveau de la connexion entre le lecteur de carte 3 et l'ordinateur 1, l'enveloppe électronique signée ainsi que représentée en figure 5a, peut être munie de manière particulièrement avantageuse d'une signature de la transaction courante entre les ressources cryptographiques auxiliaires externes, c'est-à-dire l'ensemble lecteur de carte 3, carte à microprocesseur 3a, représenté en figure 4, et l'ordinateur 1. Cette signature peut être réalisée à partir de la transaction courante et d'une valeur unique engendrée par les ressources cryptographiques auxiliaires, c'est-à-dire par la carte à microprocesseur 3a. A titre

d'exemple non limitatif, on indique que la valeur unique peut être une valeur horaire ou, de préférence, une valeur de date donnée en temps réel, c'est-à-dire selon le format année, mois, jour, heure, minute, seconde, le cas échéant centième de seconde. Dans ces conditions, on comprend que la carte à microprocesseur n'étant dotée que de ressources système peu élaborées, la transaction entre la carte à microprocesseur 3a, par l'intermédiaire du lecteur de carte 3 et l'ordinateur 1, peut être établie de façon à comporter une étape préliminaire consistant, préalablement au transfert de la transaction précitée entre la carte à microprocesseur 3a et le micro-ordinateur 1, à effectuer le calcul de la valeur unique précitée dans le format précédemment mentionné. La signature de la transaction et de la valeur unique précitée peut alors être effectuée au niveau de la carte à microprocesseur 3a grâce au module cryptographique dont celle-ci est normalement équipée. Sur la figure 5a, on a noté la valeur de signature, désignée par signature anti-rejeu SAR, comme un champ supplémentaire ajouté à l'enveloppe électronique signée ES.

Lors de la réception par l'utilisateur de l'ensemble constitué par la concaténation des données chiffrées, c'est-à-dire de l'ensemble CE et de l'enveloppe électronique ES telle que représentée en figure 5a, ce dernier, par vérification de la signature anti-rejeu SAR, est alors en mesure de vérifier que la transmission des données chiffrées, et de manière plus précise, le chiffrement de ces données ont été effectués en l'absence de toute attaque par rejeu par un tiers non habilité.

Enfin, le système objet de la présente invention peut avantageusement être muni d'une protection ayant pour

objet d'inhiber toute tentative de clonage de la carte à microprocesseur 3.

Par carte clonée, on entend la création illicite d'une carte à microprocesseur factice, mais opérationnelle, dans laquelle les données usager de la carte à microprocesseur d'origine sont dupliquées en dehors de tout code confidentiel, ainsi que les données relatives à la fabrication. Il s'agit en particulier de données qui sont mémorisées en dehors de la mémoire à accès protégé de la carte à microprocesseur. Bien entendu, le clonage peut également consister à dupliquer des données enregistrées dans la zone mémoire à accès protégé du microprocesseur par accès frauduleux, ces données pouvant alors consister en le code confidentiel attribué à la carte à microprocesseur lors de la personnalisation de cette dernière par le fabricant.

Dans ce but, la carte à microprocesseur peut être munie, au moyen d'un verrou logique, d'une variable logique, notée F, de première utilisation mémorisée dans la carte à microprocesseur précitée.

Ainsi que représenté en figure 5b, le système objet de la présente invention comprend un module logiciel comprenant un module 4 permettant d'assurer la discrimination de la valeur de la variable logique F. Cette discrimination peut être effectuée par accès en lecture à la zone mémoire de la carte contenant la variable logique F précitée. Il comprend également un module 5 permettant, selon la valeur de la variable logique F=0 précitée, d'allouer à cette variable la valeur F=1, un module 6 de calcul d'une première valeur d'identification k de la carte à microprocesseur, présumée connue de la clé physique de

protection, et un module 7 de calcul d'une deuxième valeur d'identification k' de la clé physique de protection présumée connue de la carte à microprocesseur. Les modules 6 et 7 reçoivent des valeurs paramètres n et b nombres premiers, une valeur aléatoire ALEA permettant de calculer la première valeur k et la deuxième valeur k' d'identification. Un module 8 de comparaison des valeurs d'identification k et k' précitées permet de lancer la commande d'un module 9 d'interruption/non-interruption du processus de sécurisation, en fonction du résultat de la comparaison des valeurs d'identification k et k', ainsi qu'il sera décrit ci-après dans la description.

Selon un aspect remarquable du système objet de la présente invention, à la variable logique F est attribuée une première valeur logique F=0 antérieurement à toute première utilisation de la carte à microprocesseur considérée pour effectuer une sécurisation de données.

Au contraire, une deuxième valeur logique permanente F=1, valeur complémentée de la première valeur logique F=0, est attribuée dès la première utilisation de la carte à microprocesseur afin de procéder à la sécurisation des données après que cette première utilisation ait été validée compte tenu de la valeur K du code de la clé physique de protection. On comprend en particulier que cette première utilisation, et bien entendu les utilisations ultérieures, du système objet de la présente invention, c'est-à-dire de l'ensemble constitué par le micro-ordinateur 1, la clé physique de protection 2 et l'ensemble constitué par le lecteur de carte 3 et la carte à microprocesseur 3a, ne peut être réalisée qu'avec la clé physique de protection dédiée, allouée au système préci-

tée. Ainsi, la deuxième valeur logique F=1, valable pour toutes les utilisations ultérieures à partir de la première utilisation et au-delà, permet de configurer la carte à microprocesseur 3a selon une carte à microprocesseur liée à la clé physique de protection dont le code dédié K a été reconnu.

Selon un aspect particulièrement remarquable du système objet de la présente invention, celui-ci comporte également un module générateur d'une première valeur d'identification k de la carte à microprocesseur, cette valeur d'identification étant présumée connue de la clé physique.

De même, le système objet de la présente invention, comporte un module générateur d'une deuxième valeur k' d'identification de la clé physique présumée connue de la carte à microprocesseur.

La première et la deuxième valeur d'identification k et k' sont obtenues à partir d'un aléa A engendré par le générateur aléatoire précédemment mentionné dans la description, cet aléa A étant mémorisé, d'une part, dans la clé physique de protection à titre de valeur commune pour la clé physique de protection et pour la carte à microprocesseur.

Ainsi, compte tenu de la valeur de l'aléa A commune précitée, la première valeur d'identification k de la carte à microprocesseur est présumée connue de la clé physique de protection dans la mesure où le recalcul de la deuxième valeur d'identification k' de la clé physique de protection, présumée connue de la carte à microprocesseur, est égale à la valeur k et réciproquement.

Le mode opératoire de l'ensemble est représenté en figure 5c dans deux situations distinctes, une première situation correspondant à une situation antérieure à la première utilisation de la carte à microprocesseur, soit pour F=0, et une deuxième situation correspondant à toute utilisation ultérieure comprenant la première et toutes les utilisations successives de la carte à microprocesseur pour assurer une sécurisation de données.

L'opération de lecture de la variable F à l'étape 7000 est suivie d'un test de comparaison de la valeur de F à la valeur 0 à l'étape 7001.

Pour toute variable logique de première utilisation F égale à la première valeur logique F=0, la carte à microprocesseur d'origine et la carte clonée sont indifférenciées préalablement à une première utilisation et sont donc sensiblement équivalentes. En effet, dans une telle situation, on ne sait pas discriminer a priori, informatiquement parlant, et donc fonctionnellement parlant, la carte à microprocesseur d'origine de la carte clonée. Dans cette situation, après l'étape 7001, une valeur aléatoire A, l'aléa précédemment mentionné, est engendrée à l'étape 7002, cette étape 7002 étant suivie d'une étape 7003 de mémorisation de l'aléa A dans la clé physique de protection. Les étapes 7002 et 7003 sont suivies d'une étape 7004 consistant à calculer la première valeur d'identification k de la carte à microprocesseur susceptible d'être connue de la clé physique de protection. A titre d'exemple illustratif, la première valeur d'identification k peut consister en la valeur réduite modulo n de l'aléa A multipliée par un nombre arbitraire b donné. A titre d'exemple

non limitatif, la première valeur d'identification peut vérifier la relation :

$$K = (A \text{ Mod } n).b$$

L'étape 7004 précitée est alors suivie d'une étape 7005 de mémorisation de la valeur de k dans la carte à microprocesseur et en particulier dans la zone mémoire à accès protégé de cette dernière. Les étapes 7004 et 7005 sont alors suivies d'une étape 7006 consistant à mémoriser dans la carte à microprocesseur 3a la valeur de la variable logique F de première utilisation instanciée à la valeur 1, F=1. L'étape 7006 est alors suivie d'une étape 7007 consistant à mémoriser la valeur de la variable logique F dans la carte à microprocesseur, puis d'une étape 7008 générale, permettant la poursuite de la sécurisation des données grâce au système objet de la présente invention.

Au contraire, suite à l'étape de test 7001 de la variable logique de première utilisation F et pour la valeur 1 de cette dernière, la variable logique de première utilisation étant égale à la deuxième valeur logique, la carte à microprocesseur 3a d'origine et la carte clonée sont indifférenciées préalablement à une utilisation ultérieure à une première utilisation, mais non équivalentes pour les raisons qui seront explicitées ci-après.

Dans cette situation, l'étape de test 7001 est suivie d'une étape 7009 de lecture de la valeur de l'aléa A mémorisée dans la clé physique de protection. L'étape 7009 est elle-même accompagnée d'une étape 7010 consistant à effectuer une lecture de la première valeur d'identifi-

cation k dans la carte à microprocesseur. L'étape 7009 est suivie d'une étape 7011 consistant à calculer la deuxième valeur d'identification k' de la clé physique présumée connue de la carte à microprocesseur, la valeur k' vérifiant la relation :

$$k' = (A \text{ Mod } n).b$$

Les étapes 7010 et 7011 sont suivies d'une étape 7012 consistant à comparer l'égalité de la première et la deuxième valeur d'identification par comparaison d'égalité $k = k'$.

Sur réponse positive au test de comparaison 7012 à la comparaison d'égalité, la carte à microprocesseur est liée à la clé physique, et réciproquement. En effet, carte à microprocesseur et clé physique, disposaient de la valeur du même aléa A et étaient donc liées par cette même valeur. Dans une telle situation, un processus de régénération des première et deuxième valeurs d'identification k et k' est réalisé par une étape 7015 consistant à engendrer un nouvel aléa, noté ALEA = A', lequel bien entendu est réputé différent de l'aléa A. Le nouvel aléa A' est alors mémorisé en une étape 7016 dans la clé physique de protection. En outre, une étape 7017 est prévue, laquelle permet de calculer la nouvelle valeur de la première valeur d'identification k à l'étape 7017 selon la relation :

$$k = (A' \text{ Mod } n).b$$

On comprend en fait que grâce à la mise en œuvre des étapes 7015, 7016 et 7017, puis grâce à la mémorisa-

tion de la première valeur d'identification k régénérée à l'étape 7017, la première valeur d'identification de la carte à microprocesseur k, présumée connue de la clé physique de protection, a été explicitement régénérée, alors que la mémorisation du nouvel aléa A' dans la clé physique de protection à l'étape 7016 permet une régénération implicite de la deuxième valeur d'identification de la clé physique de protection présumée connue de la carte à microprocesseur lors de la mise en œuvre ultérieure d'une session de sécurisation de données distinctes. L'étape 7018 est alors suivie d'une étape 7019 consistant à effectuer une poursuite de la sécurisation des données considérées.

Au contraire, sur réponse négative à l'étape 7012 de comparaison des première et deuxième valeurs d'identification k et k', la carte à microprocesseur et la clé physique de protection ne sont pas liées en raison du fait qu'elles ne disposent pas de la même valeur d'aléa A. Dans ce cas, une étape 7014 est prévue, laquelle provoque la sortie du programme de sécurisation, le système objet de la présente invention étant mis hors service pour l'utilisateur frauduleux de la carte non liée, c'est-à-dire de la carte clonée.

Les modules générateurs de la première et de la deuxième valeur d'identification k et k' peuvent être constitués par un module générateur d'une valeur aléatoire et par un module de calcul permettant de calculer ces valeurs d'identification sous forme de valeurs réduites modulo n de la valeur aléatoire considérée, n désignant un nombre premier et b un nombre arbitraire tel qu'un nombre premier également par exemple.

En résumé, en cas de clonage quasi parfait des cartes à microprocesseur pour une valeur de variable logique de première utilisation F=0, la carte à microprocesseur d'origine et la carte à microprocesseur clonée étant indifférenciées et équivalentes, la première carte utilisée, originale ou clone quasi parfait, est liée durant son cycle de vie à la clé physique de protection à laquelle elle devient dédiée.

Toute autre carte telle que l'originale ou un autre clone ne peut être utilisée à moins de disposer d'autres clés physiques de protection valides.

En effet, dans le cas de clonage quasi parfait des cartes à microprocesseur munies d'une variable logique de valeur de première utilisation F=1, l'usage de la carte originale interdit l'utilisation de la carte à microprocesseur clonée, quasi parfaite, pour les raisons précédemment mentionnées dans la description. Par contre, l'usage de la carte clonée quasi parfaite rend également inutilisable la carte originale.

Ainsi, vu de l'administrateur réseau habilité ou du gestionnaire de ce réseau, une seule et unique carte liée est utilisée, la carte liée pouvant être soit l'originale, soit le clone quasi parfait.

La carte à microprocesseur originale et les clones quasi parfaits peuvent alors être invalidées, soit par la date de validité de la carte, soit par les bornes de contrôle et bornes temporelles de la clé physique de protection.

REVENDICATIONS

1. Procédé de sécurisation de données numériques traitées par un ordinateur, cet ordinateur étant muni d'une clé physique de protection permettant de délivrer à cet ordinateur un code de clé physique et des valeurs spécifiques de paramétrage cryptographique, caractérisé en ce que ce procédé consiste, pour tout ensemble de données numériques traitées par cet ordinateur :

- à chiffrer cet ensemble de données à partir d'au moins une clé de chiffrement, pour engendrer un ensemble de données chiffrées ;

- à associer à cet ensemble de données chiffrées une enveloppe électronique signée comportant au moins des paramètres non chiffrés tels que :

- un aléa de p bits ;
- un motif d'identification d'enveloppe électronique signée, codé sur S bits, ce motif d'identification étant calculé à partir d'au moins une des valeurs spécifiques de paramétrage cryptographique et permettant de vérifier l'existence d'un ensemble de données chiffrées associé à cette enveloppe électronique signée ;
- un numéro représentatif de ladite clé physique de protection équipant ledit ordinateur ;
- une signature électronique conjointe, obtenue à partir d'une signature dudit ensemble de données chiffrées et d'une signature des paramètres non chiffrés de ladite enveloppe électronique, ce qui permet lors de l'utilisation desdites données chiffrées de cet ensemble de données chiffrées de procéder à une vérification de l'authenticité des paramètres non chiffrés de ladite enveloppe électronique signée, de l'intégrité de l'en-

semble des données chiffrées et de l'enveloppe électronique signée, puis de déchiffrer lesdites données chiffrées de cet ensemble de données chiffrées pour utilisation.

2. Procédé selon la revendication 1, caractérisé en ce que lesdits paramètres non chiffrés comportent en outre un bit indicateur du mode d'utilisation local, monoposte, au niveau dudit ordinateur, respectivement distant, en réseau, multiposte, desdites données chiffrées.

3. Procédé selon les revendications 1 et 2, caractérisé en ce que, pour une utilisation en mode distant, lesdits paramètres non chiffrés comportent en outre un code détecteur correcteur d'erreurs permettant, après transmission, une vérification de l'intégrité des données chiffrées et signées transmises.

4. Procédé selon l'une des revendications 2 ou 3, caractérisé en ce que, pour une utilisation en mode distant, lesdits paramètres non chiffrés comportent en outre un code d'identification de l'expéditeur de cet ensemble de données chiffrées, ce qui permet de procéder à une vérification de non-répudiation de cet expéditeur.

5. Procédé selon l'une des revendications 2 à 4, caractérisé en ce que, pour une utilisation en mode distant, lesdits paramètres non chiffrés comportent en outre un code d'identification du destinataire de cet ensemble de données chiffrées, ce qui permet d'assurer un acheminement sélectif desdites données chiffrées en fonction du code d'identification du destinataire et des droits attribués à ce dernier, l'opération de déchiffrement de ces données chiffrées, par ce destinataire, permettant de prouver la validité de cet acheminement sélectif.

6. Procédé selon l'une des revendications précédentes, caractérisé en ce que lesdits paramètres non chiffrés comportent en outre une valeur de date temps réel de ladite opération de chiffrement.

7. Procédé selon l'une des revendications 1 à 6, caractérisé en ce que ladite signature conjointe consiste en une opération de signature consistant à :

- calculer une signature externe sur n octets dudit ensemble de données chiffrées à partir de ressources cryptographiques auxiliaires audit ordinateur ;

- calculer une signature interne sur n octets desdits paramètres non chiffrés de ladite enveloppe électronique à partir d'un processus cryptographique à clé secrète ;

- effectuer une opération de combinaison logique OU exclusif bit à bit entre ladite signature externe et ladite signature interne.

8. Procédé selon l'une des revendications 1 à 7, caractérisé en ce que ladite opération consistant à chiffrer cet ensemble de données pour engendrer un ensemble de données chiffrées consiste :

- à engendrer une suite chiffrante à partir d'un générateur pseudo-aléatoire, ladite suite chiffrante constituant ladite au moins une clé de chiffrement ;

- à effectuer une combinaison logique OU exclusif d'octet à octet entre ledit ensemble de données et ladite suite chiffrante, pour engendrer ledit ensemble de données chiffrées.

9. Procédé selon les revendications 7 et 8, caractérisé en ce que l'étape consistant à engendrer ladite suite chiffrante consiste :

- à choisir dans ledit ensemble de données numériques, préalablement à l'opération de chiffrement, un premier (A) et un deuxième (B) mot ;

- à sélectionner parmi les données de ladite carte à microprocesseur un premier et un deuxième mot de référence de même taille en nombre d'octets que le premier et le deuxième mot respectivement ;

- à former par combinaison logique de type OU exclusif octet à octet du premier mot et du premier mot de référence, respectivement du deuxième mot et du deuxième mot de référence, une première et une deuxième clé virtuelle ;

- à engendrer ladite suite chiffrante à partir desdites clés virtuelles et de polynômes générateurs.

10. Procédé selon la revendication 9, caractérisé en ce que l'opération de chiffrement de l'ensemble des données numériques consiste, à partir de ladite suite chiffrante :

- à remplacer lesdits premier (A) et deuxième (B) mots de cet ensemble de données numériques par la première respectivement la deuxième clé virtuelle pour engendrer un ensemble de données numériques incrusté ;

- à soumettre à l'opération de chiffrement ledit ensemble de données numériques incrusté, à l'exception des première et deuxième clés virtuelles incrustées, pour engendrer ledit ensemble de données chiffrées.

11. Procédé selon la revendication 9 ou 10, caractérisé en ce que, lors de l'utilisation, pour assurer le déchiffrement des données chiffrées de cet ensemble de données chiffrées, celui-ci consiste :

- à discriminer dans ledit ensemble de données chiffrées lesdites première et deuxième clés virtuelles incrustées ;

- à restituer, à partir desdites données de ladite carte à microprocesseur et du premier et du deuxième mot de référence, par combinaison logique de type OU exclusif lesdits premier (A) et deuxième (B) mots ;

- à restituer, à partir desdites clés virtuelles, ladite suite chiffrante ;

- à remplacer, dans lesdites données chiffrées de l'ensemble de données chiffrées, lesdites clés virtuelles par le premier (A) respectivement le deuxième (B) mot, pour restituer un ensemble de données numériques chiffrées modifié ;

- à soumettre ledit ensemble de données numériques chiffrées modifié à un processus de déchiffrement, à partir de ladite suite chiffrante, à l'exception desdits premier et deuxième mots, ce qui permet de restituer les données numériques dudit ensemble de données numériques pour l'utilisation.

12. Système de sécurisation de données numériques traitées par un ordinateur, cet ordinateur étant muni d'une clé physique de protection permettant de délivrer à cet ordinateur un code de clé physique et des valeurs spécifiques de paramétrage cryptographique, caractérisé en ce que ledit système comporte en outre :

- des moyens de chiffrement de cet ensemble de données à partir d'au moins une clé de chiffrement, pour engendrer un ensemble de données chiffrées ;

- des moyens de calcul, à partir de cet ensemble de données chiffrées, d'une enveloppe électronique signée

comportant au moins des paramètres non chiffrés tels qu'un aléa de p bits, un motif d'identification d'enveloppe électronique signée codé sur S bits, ce motif d'identification étant calculé à partir d'au moins une des valeurs spécifiques de paramétrage cryptographique et permettant de vérifier l'existence d'un ensemble de données chiffrées associé à cette enveloppe électronique signée, un numéro représentatif de ladite clé physique de protection équipant ledit ordinateur une signature électronique conjointe obtenue à partir d'une signature dudit ensemble de données chiffrées et d'une signature des paramètres non chiffrés de ladite enveloppe électronique ;

- des moyens de concaténation dudit ensemble de données chiffrées et de ladite enveloppe électronique signée, pour engendrer lesdites données sécurisées, ce qui permet, lors de l'utilisation locale ou distante desdites données chiffrées de cet ensemble de données chiffrées, de procéder à une vérification de l'authenticité des paramètres non chiffrés de ladite enveloppe électronique signée, de l'intégrité de l'ensemble des données chiffrées et de l'enveloppe électronique signée puis de déchiffrer lesdites données chiffrées de cet ensemble de données chiffrées pour utilisation.

13. Système selon la revendication 12, caractérisé en ce que lesdits moyens de chiffrement de cet ensemble de données pour engendrer un ensemble de données chiffrées comportent :

- des moyens générateurs d'une suite chiffrante comprenant un générateur pseudo-aléatoire, ladite suite chiffrante constituant ladite au moins une clé de chiffrement ;

- des moyens de combinaison logique OU exclusif d'octet à octet entre ledit ensemble de données et ladite suite chiffrante, pour engendrer ledit ensemble de données chiffrées.

14. Système selon l'une des revendications 12 ou 13, caractérisé en ce que lesdits moyens de calcul, à partir de cet ensemble de données chiffrées, d'une enveloppe électronique signée comprenant au moins, en vue de calculer ladite signature électronique conjointe :

- des moyens de calcul d'une signature externe sur n octets dudit ensemble de données chiffrées, lesdits moyens de calcul consistant en des ressources cryptographiques auxiliaires externes audit ordinateur ;

- des moyens de calcul d'une signature interne sur n octets desdits paramètres non chiffrés de ladite enveloppe électronique, à partir d'un processus cryptographique à clé secrète ;

- des moyens de combinaison logique OU exclusif bit à bit entre ladite signature externe et ladite signature interne permettant d'engendrer ladite signature électronique conjointe.

15. Système selon la revendication 14, caractérisé en ce que lesdites ressources cryptographiques auxiliaires sont constituées par :

- une carte à microprocesseur munie de ressources cryptographiques ;

- une interface de carte à microprocesseur connectée audit ordinateur.

16. Système selon les revendications 13, 14 et 15, caractérisé en ce que lesdits moyens générateurs d'une suite chiffrante comportent :

- des moyens de sélection, dans ledit ensemble de données numériques, d'un premier et d'un deuxième mot ;

- des moyens de sélection, dans ladite carte à microprocesseur, d'un premier et d'un deuxième mot de référence de même taille en nombre d'octets que le premier et le deuxième mot ;

- des moyens de calcul, à partir du premier mot et du premier mot de référence, respectivement du deuxième mot et du deuxième mot de référence, d'une première et d'une deuxième clé virtuelle ;

- des moyens de lecture de polynômes générateurs, et

- des moyens de calcul à partir desdits polynômes générateurs et desdites clés virtuelles de ladite suite chiffrante.

17. Système selon l'une des revendications 12 à 15, caractérisé en ce que, dans le but d'inhiber toute attaque par rejeu de ce système par un utilisateur non habilité ayant procédé à une recopie de transactions entre lesdites ressources cryptographiques auxiliaires externes audit ordinateur et ledit ordinateur, ladite enveloppe électronique signée comporte en outre une signature de la transaction courante entre lesdites ressources cryptographiques auxiliaires externes audit ordinateur et ledit ordinateur et d'une valeur unique engendrée par lesdites ressources cryptographiques auxiliaires.

18. Système selon les revendications 12, 14 et 15, caractérisé en ce que dans le but d'inhiber toute tentative de clonage de ladite carte à microprocesseur, celui-ci comporte :

- des moyens de discrimination de la valeur d'une variable logique de première utilisation mémorisée dans la carte à microprocesseur, à cette variable logique étant attribuée une première valeur logique antérieurement à la première utilisation et une deuxième valeur logique permanente, valeur complémentée de cette première valeur logique, dès la première utilisation validée, compte tenu de la valeur du code de clé physique, ladite deuxième valeur logique permanente permettant de configurer ladite carte à microprocesseur selon une carte à microprocesseur liée à ladite clé physique de protection ;

- des moyens générateurs d'une première valeur d'identification de la carte à microprocesseur présumée connue de ladite clé physique ;

- des moyens générateurs d'une deuxième valeur d'identification de ladite clé physique présumée connue de la carte à microprocesseur, et pour toute variable logique de première utilisation égale à cette première valeur logique, la carte à microprocesseur d'origine et la carte clonée étant indifférenciées préalablement à une première utilisation et sensiblement équivalentes,

- des moyens d'allocation à ladite variable logique de première utilisation d'une variable égale à cette deuxième valeur logique, le processus de sécurisation de données étant poursuivi, et pour toute variable logique de première utilisation égale à cette deuxième valeur logique, la carte à microprocesseur d'origine et la carte clonée étant indifférenciées préalablement à une utilisation ultérieure à une première utilisation mais non équivalentes ;

- des moyens de comparaison d'égalité des première et deuxième valeurs d'identification, et, sur réponse positive à cette comparaison d'égalité, la carte à microprocesseur étant liée à la clé physique et réciproquement, un processus de régénération des première et deuxième valeurs d'identification et de poursuite du processus de sécurisation des données étant réalisé, et, sur réponse négative à cette comparaison d'égalité, la carte à microprocesseur n'étant pas liée à la clé physique ou réciproquement,

- des moyens d'interruption du processus de sécurisation des données.

19. Système selon la revendication 18, caractérisé en ce que les moyens générateurs d'une première valeur d'identification et les moyens générateurs d'une deuxième valeur d'identification sont constitués par :

- un module générateur d'une valeur aléatoire, cette valeur aléatoire étant inscrite dans ladite clé physique ;

- un module de calcul implanté dans ladite clé physique respectivement ladite carte à microprocesseur permettant de calculer ladite première k, respectivement deuxième k', valeur d'identification sous forme de valeur réduite modulo n de cette valeur aléatoire, n désignant un nombre premier.

2793903

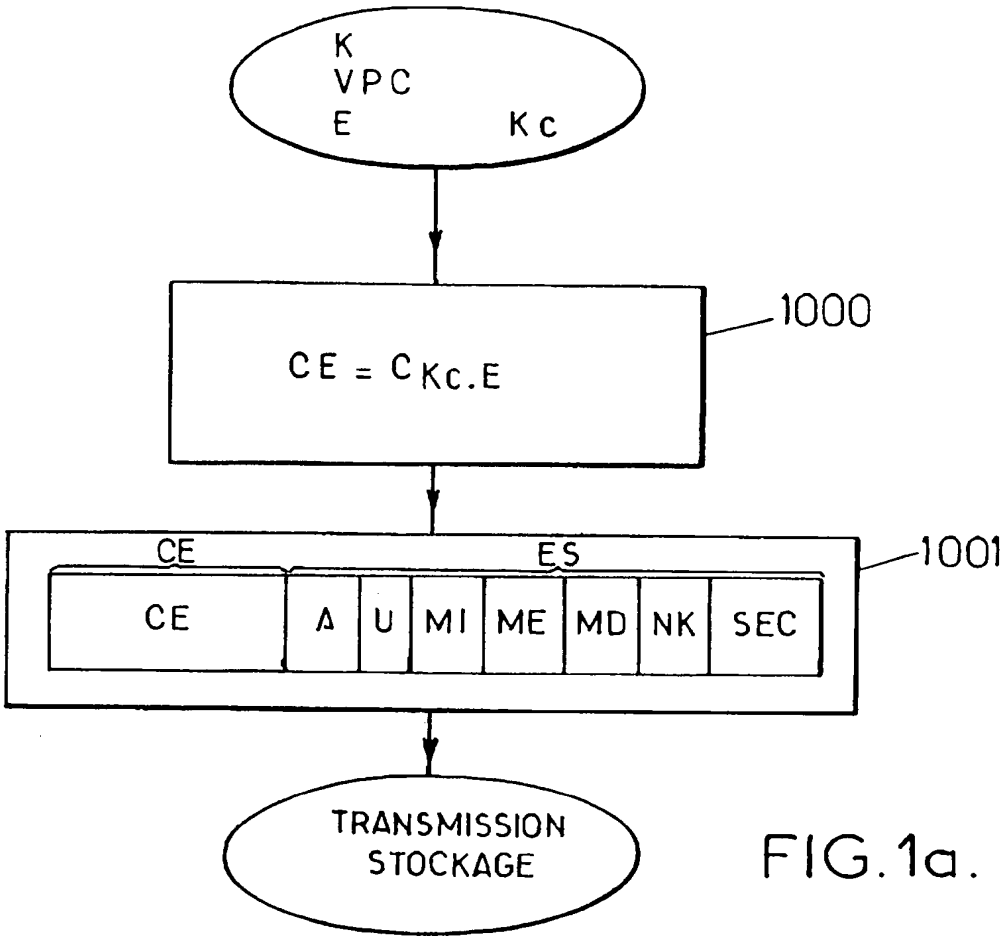
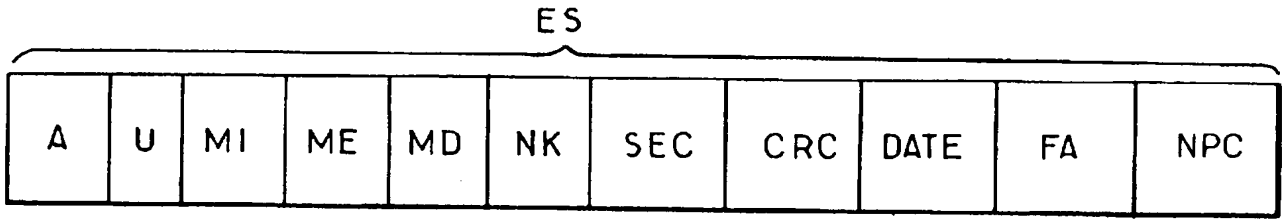


FIG.1a.



ENVELOPPE ELECTRONIQUE SIGNÉE FIG.1b.

2793903

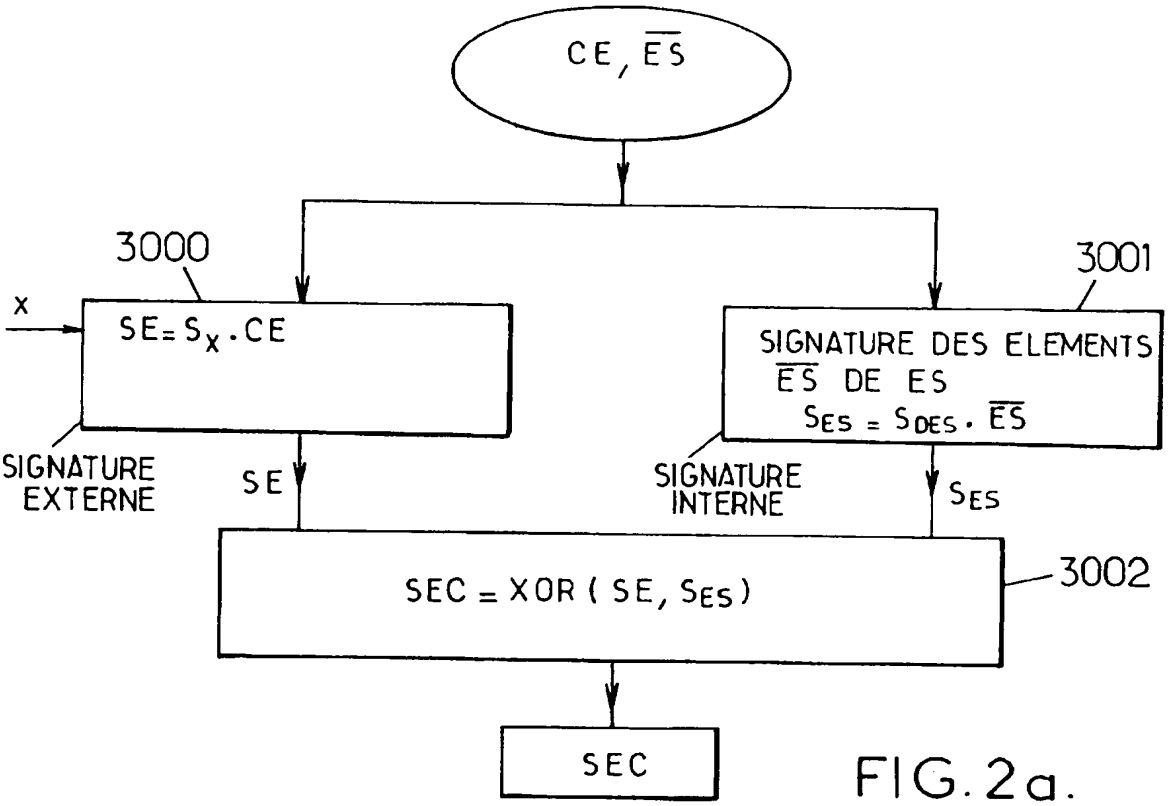


FIG. 2a.

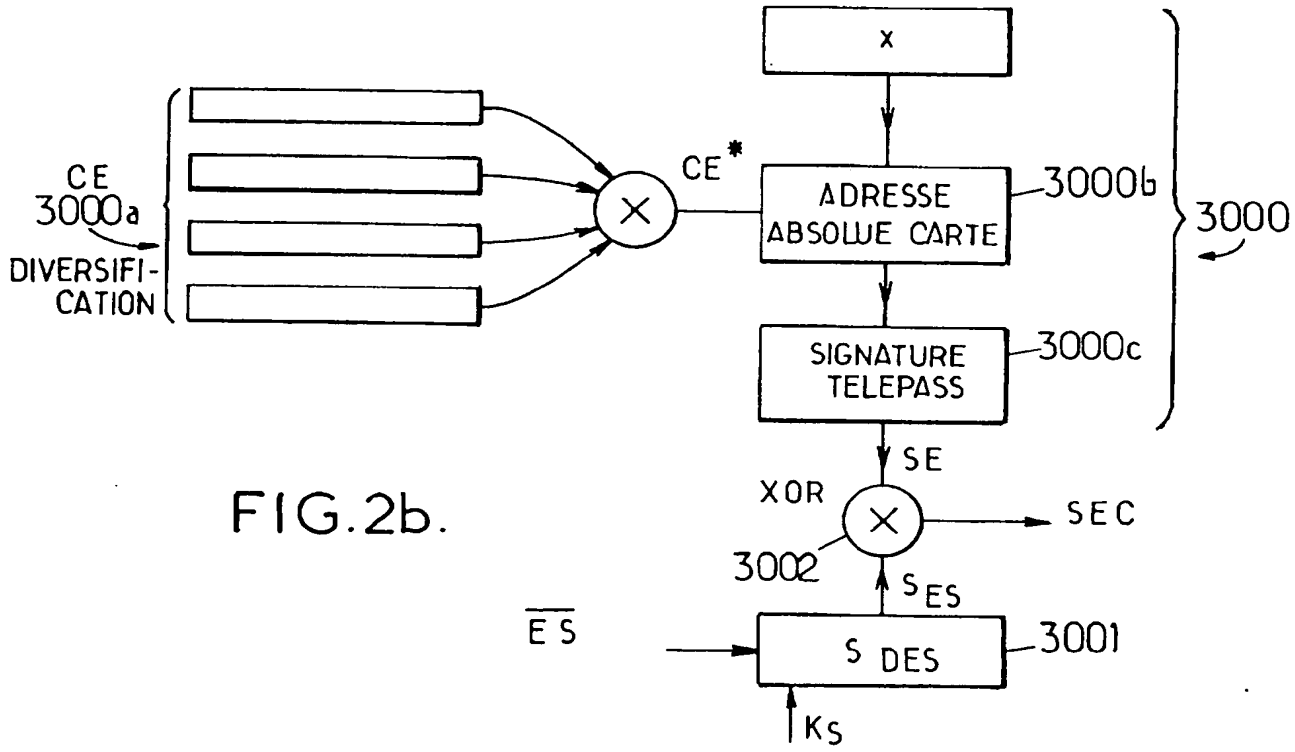


FIG. 2b.

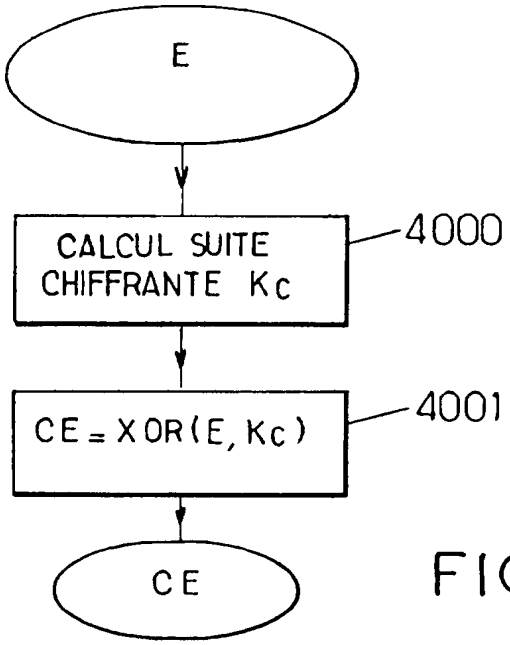


FIG. 3a.

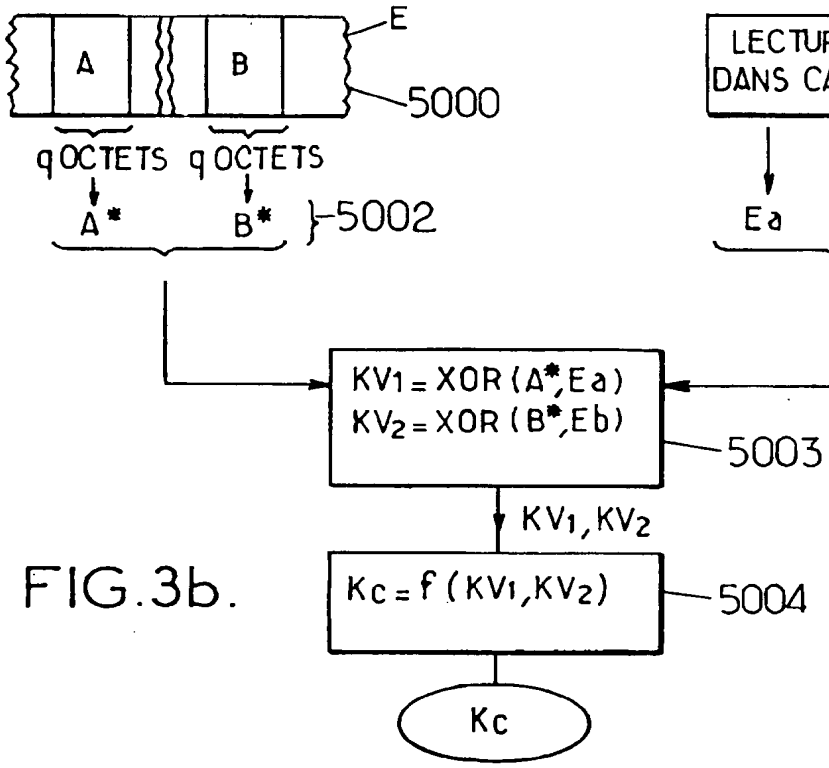


FIG. 3b.

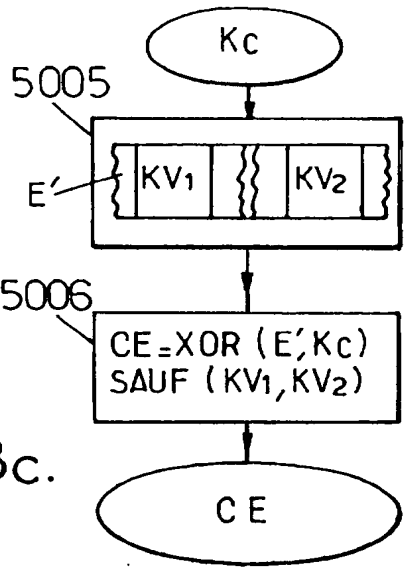


FIG. 3c.

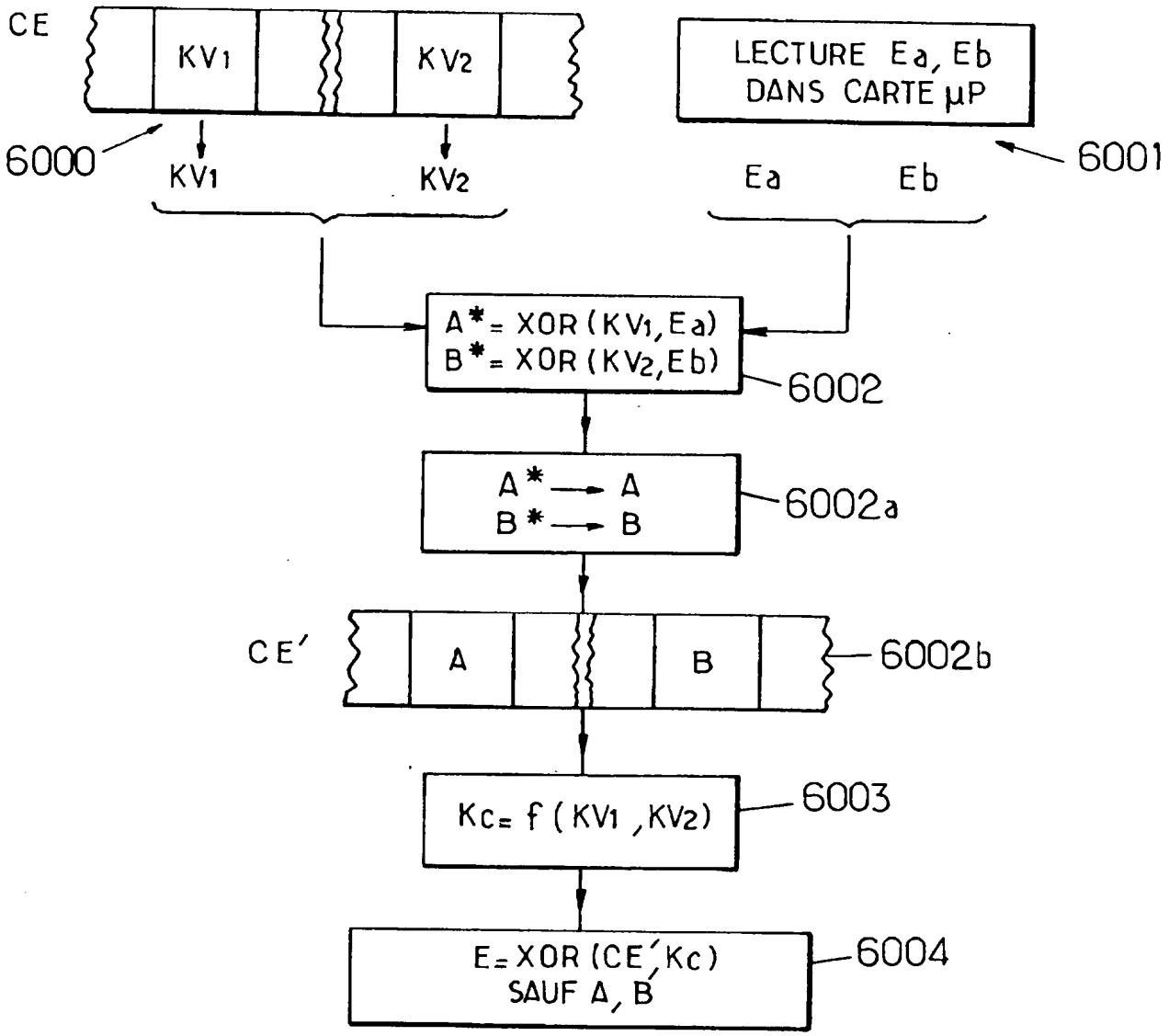


FIG.3d.

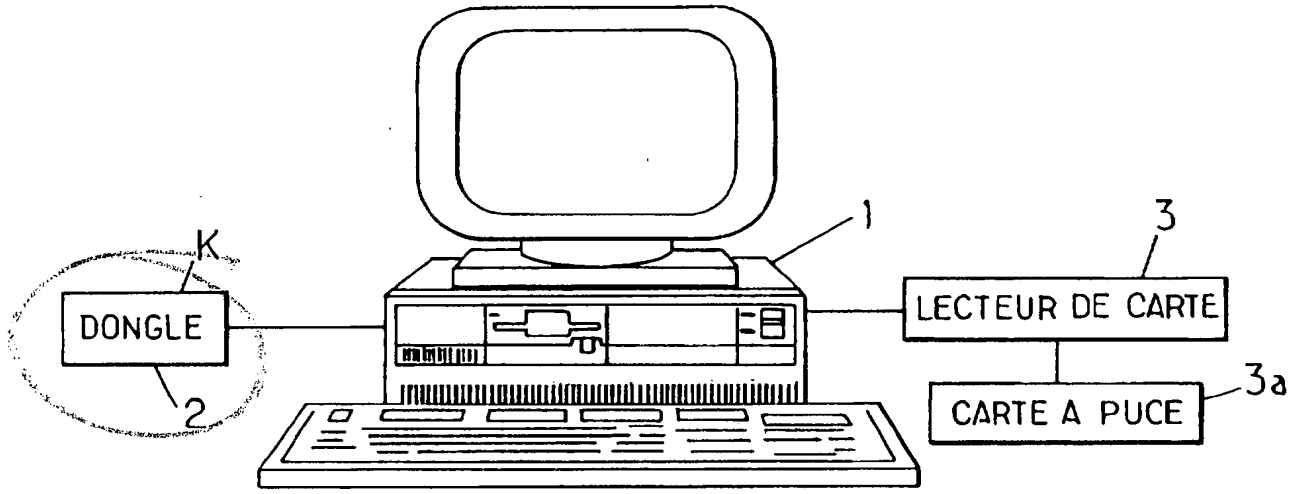


FIG.4.

A	U	MI	ME	MD	NK	SEC	CRC	DATE	FA	NPC	SAR

ENVELOPPE ELECTRONIQUE SIGNÉE
(INHIBITION ATTAQUE PAR REJEU)

FIG.5a.

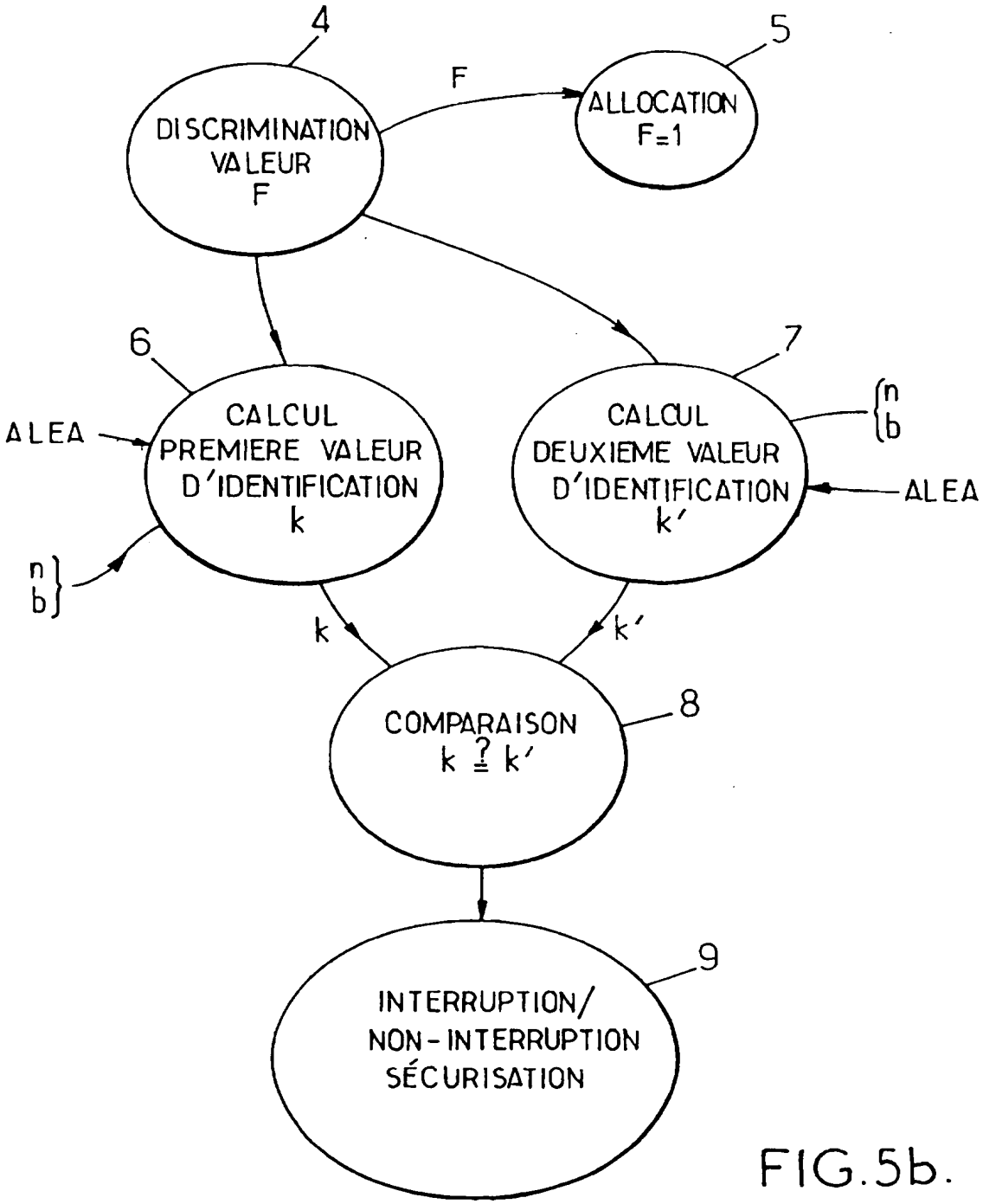


FIG.5b.

2793903

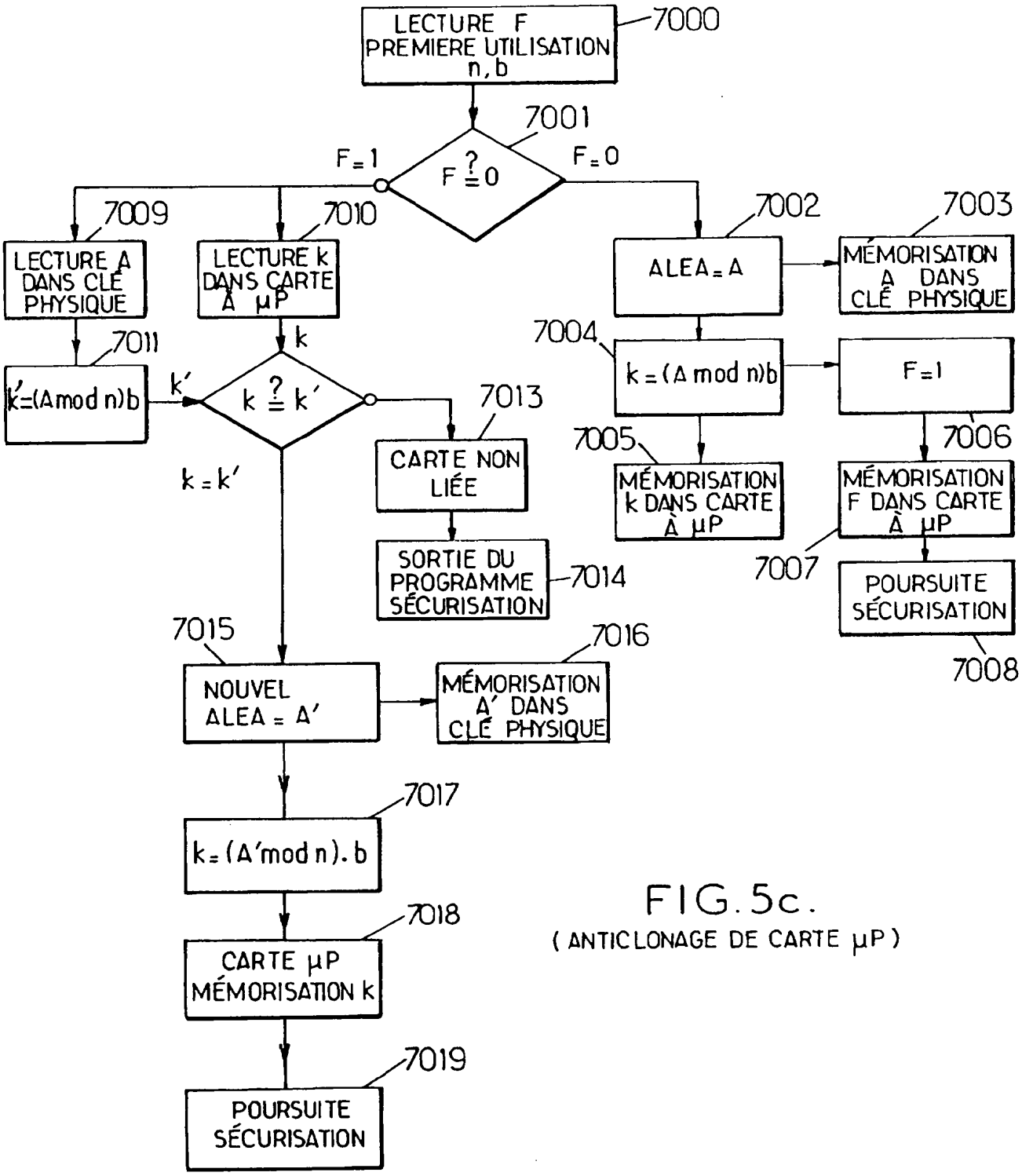


FIG. 5c.

(ANTICLONAGE DE CARTE µP)

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2793903
N° d'enregistrement national

FA 578150
FR 9906483

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
A	EP 0 537 925 A (NEWA DATACOM LTD) 21 avril 1993 (1993-04-21) * colonne 2, ligne 2 - colonne 7, ligne 50; revendications; figures *	1-19
A	FR 2 764 408 A (FRANCOIS CHARLES OBERTHUR) 11 décembre 1998 (1998-12-11) * page 1, ligne 18 - page 3, ligne 7 * * page 5, ligne 9 - page 7, ligne 24 * * page 9, ligne 31 - page 10, ligne 32; revendications; figure 1 *	1-19
A	EP 0 737 907 A (SECURE COMPUTING CORPORATION) 16 octobre 1996 (1996-10-16) * colonne 6, ligne 41 - colonne 8, ligne 9 * * colonne 11, ligne 21 - colonne 14, ligne 43 * * colonne 21, ligne 27 - colonne 24, ligne 37; revendications; figures 21,22 *	1-19

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7)

G06F
H04L

Date d'achèvement de la recherche: 23 février 2000

Examinateur: Soler, J

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

1

EPO FORM 1503 03.82 (P04C19)